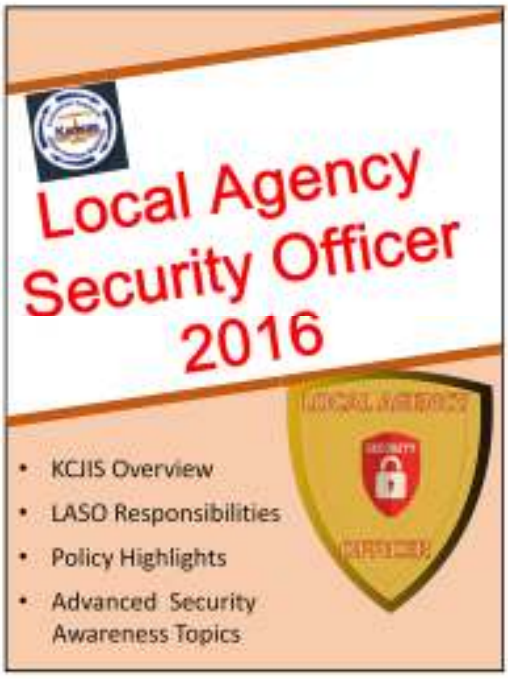


Welcome to Local Agency Security Officer training!

This course will cover:

1. A brief description of what KCJIS is.
    a. Who the main state level players are and their respective roles
    b. Some of the services available through KCJIS
2. The 6 responsibilities specifically assigned to LASOs in the KCJIS Policies and Procedures manual.
    a. And some of the resources LASOs can use to fulfill their responsibilities.
3. And then we will look at some specific policies of interest based on:
    a. Their pertinence to emerging technologies
    b. They seem to generate frequently asked questions to the CJIS unit staff.
    c. Noteworthy policy changes
    d. Policies that we need to be reminded of (gold background slides)
4. Some related higher level security awareness topics mixed in (blue slide backgrounds)
5. Some of the forms and workflows used for requesting access to KCJIS are mentioned.

Here's a quick overview of KCJIS.
Essentially the Responsibilities to manage what is KCJIS are divided between the KBI and KHP as set by statute and appointed by the governor.

As directed in Title 28 of the Code of Federal Regulations, Chapter 1, Part 20 …
state statute designates the KBI as the keeper of the statewide Computerized Criminal History records (repository).

The series of statutes beginning with 22-4701 establish:

1. The repository at the KBI.
2. Lists certain reportable events to be included in the repository.
3. Defines terms.
4. Establishes rules for dissemination of Kansas CHRI.
5. And other details.

By the way, if you read these statutes and the title 28 chapter 1 part 20, you will see some repetitive language.

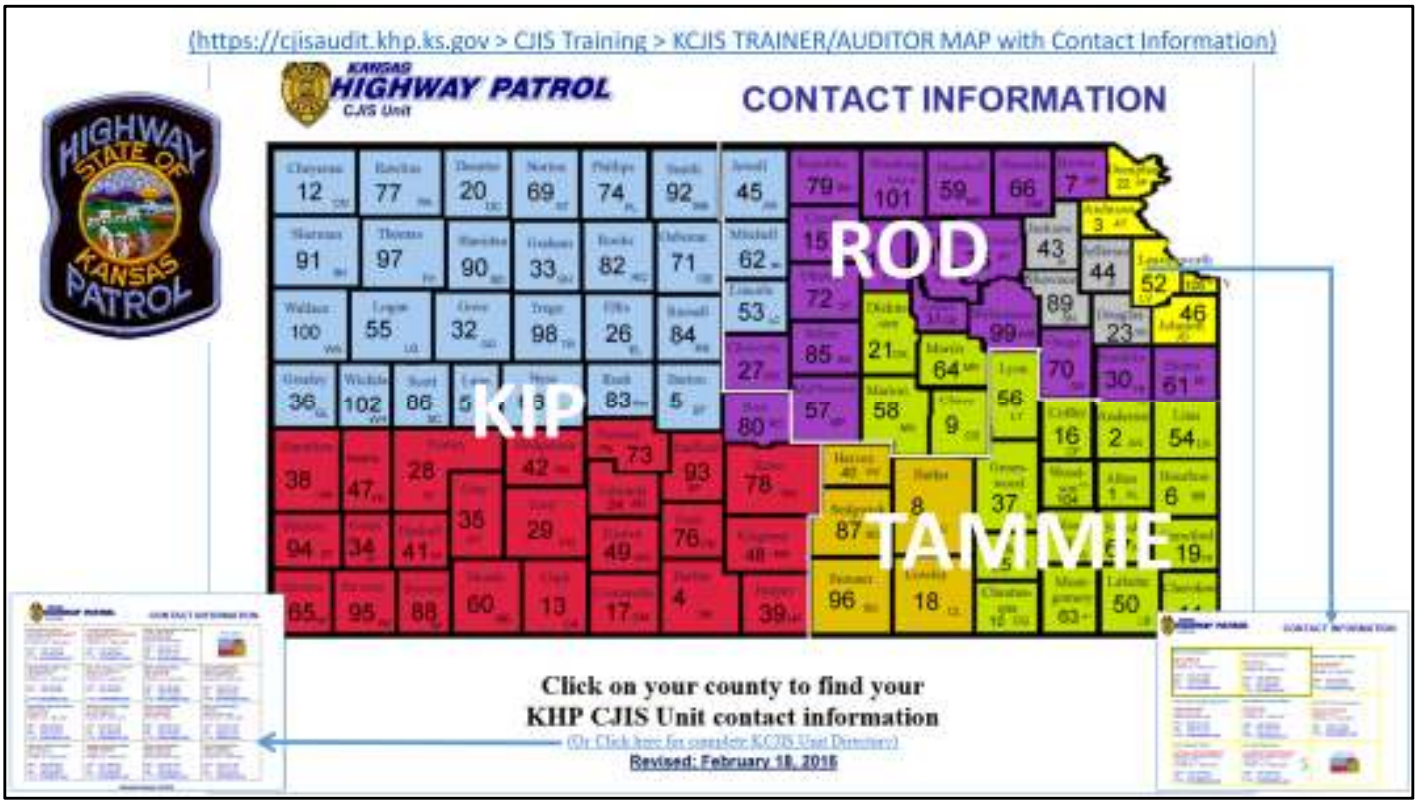
That all said, the KBI has invested in resources to carry out their responsibilities under these statutes.
As such, they host the majority of the state information within various databases and applications.
If they don't hold the information themselves, they strive to provide a pathway to it through the KCJIS portal or other means.
They continue to work to improve services and connectivity to external (other agency) systems that your agency needs to complete its mission.

The KHP has been designated by a governor some time ago as the CJIS Systems Agency for Kansas.
The KHP has the two positions required by Title 28 and FBI policies – the CJIS System Officer (CSO) and Information Security Officer (ISO).

As the CSA, the KHP is responsible for Training and auditing of NCIC, III, and N-Dex use in Kansas.
Auditing includes verifying:
DQ/NCIC
Quality of entries by local agencies into NCIC and III
Appropriate access and use of NCIC & III records
Access and Use of N-Dex

Information Technology Security
Proper security policies and procedures are in place and followed to protect the shared data in the various systems.

The ISO and staff also review requests for initial connections and additional devices and changes to and agency's KCJIS connections.



The Information Technology Security Audit (I.T.S.A.) team of the KHP CJIS Unit consist of the ISO and 3 auditors.

All of our unit's contact information is available from the CJIS training area of our KHP CJIS launch pad
(https://cjisaudit.khp.ks.gov)

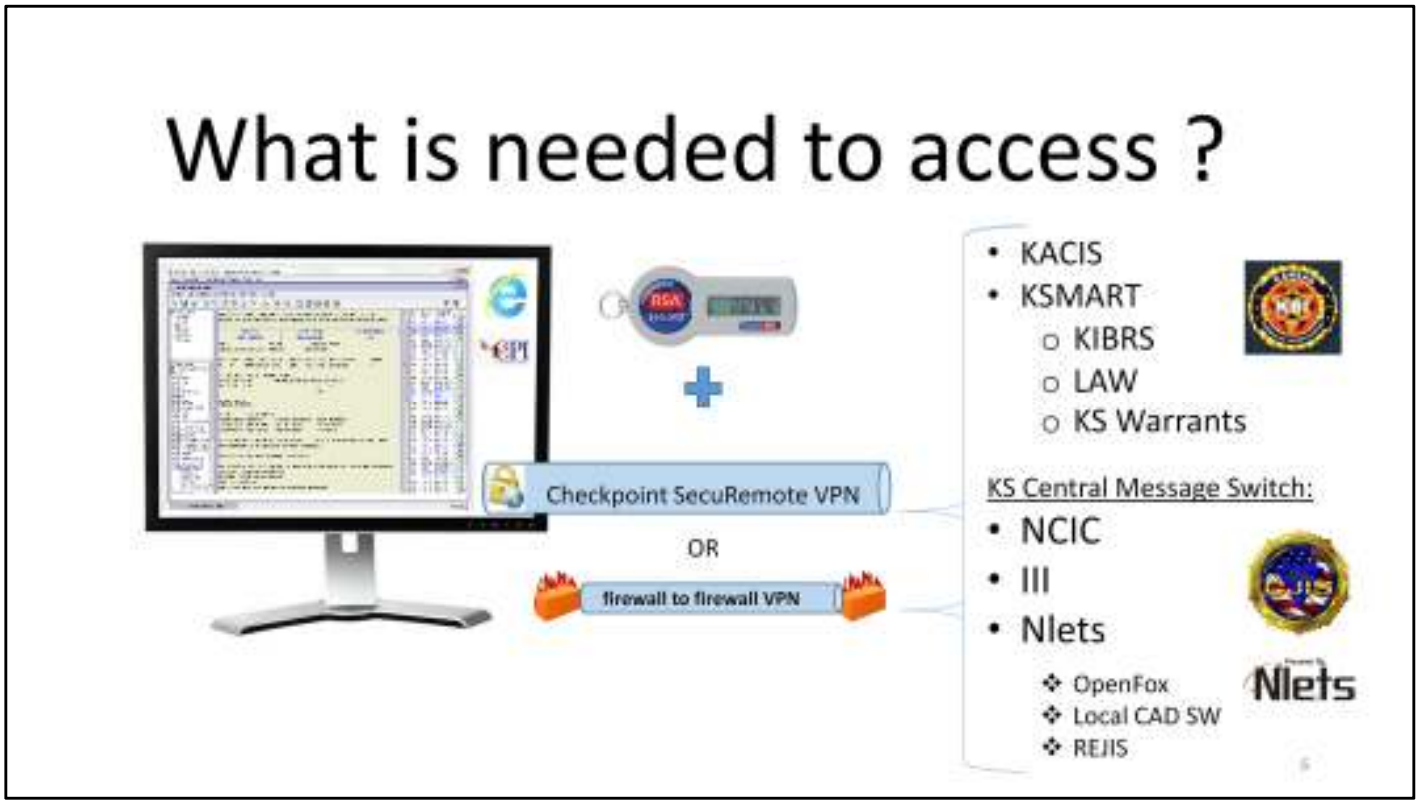
Kip Ballinger is assigned to the western part of the state.
Rod Strole is assigned to the northeastern quadrant.
Tammie Hendrix has the southeastern quadrant.

Don Cathey, the KCJIS Information Security Officer supervises these 3.

Lt. Craig Phillips is Don's boss.

Capt. Justin Bramlett replaced Randy Moon as the CSO for Kansas in spring 2015.

Randy Moon is now the KHP's Lt. Colonel.

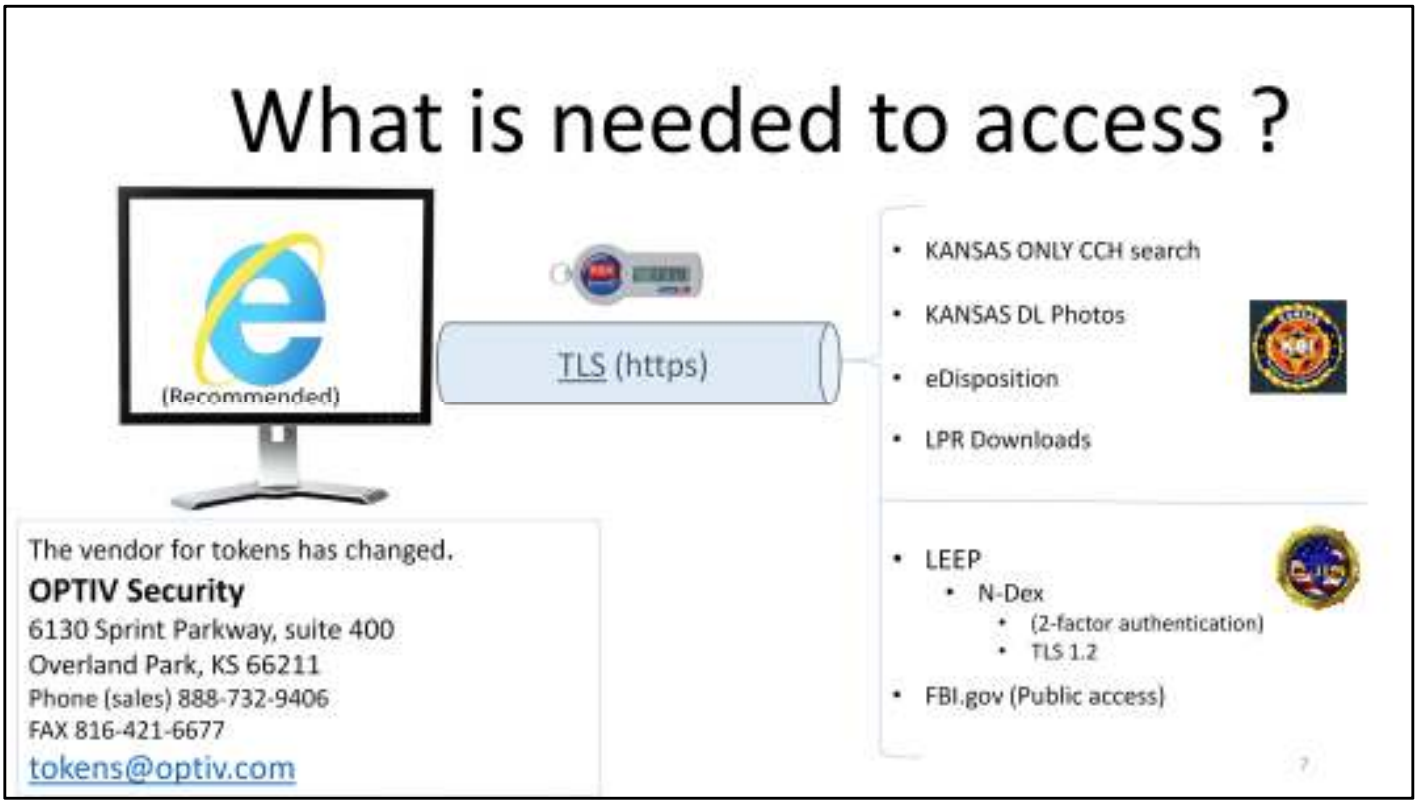


Each user from your agency will need to have a KCJIS user ID for your agency.
If they work for other agencies, they will need a user ID for them as well.

Currently, every KCJIS ***userID*** must be accompanied by a Personal Identification Number (PIN) and an RSA SecureID token as a second factor of authentication.

All KCJIS connected service programs require an encrypted connection that is certified by the National Institute of Standards and Technology (NIST) to meet the Federal Information Processing Standard (FIPS) 140-2.

The “meatier” services require a Pre-Shared Key encryption method.
Either the state supplied Checkpoint SecuRemote Virtual Private Network (VPN) client installed on each device,
Or a firewall to firewall VPN a.k.a Site to Site VPN that is established through cooperation of your I.T. and the KBI security office.

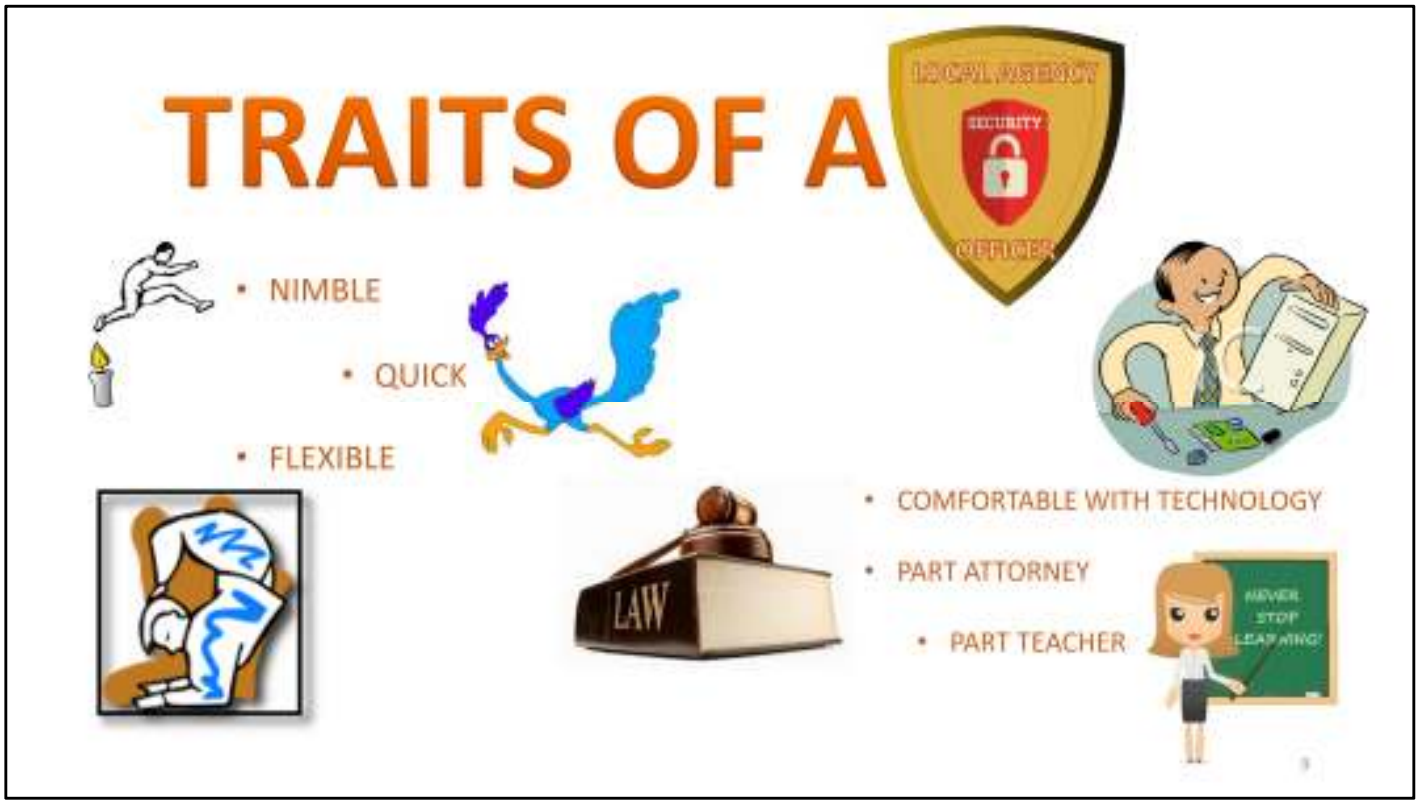


Some programs are available to KCJIS users through Microsoft Internet Explorer 11 (the only browser supported by the KBI).
The KCJIS portal and other KCJIS resources use Transport Layer Security (TLS) - denoted in the web address by https - to encrypt traffic between the user's computer and KCJIS.

Be sure the "Use TLS 1.0 through 1.2 …" boxes are checked in your Internet Explorer's
Internet Options
Advanced settings
Security

TLS is also used by the FBI.
LEEP requires TLS 1.2 (the latest) for access through your browser.

Additional informational resources are publicly available from FBI.gov (more on this later).



This slide represents some human characteristics that have proven beneficial to LASOs .

Jack was nimble, he was quick. He could jump over candle sticks!
The roadrunner was quick – fast off the start but can stop on a dime. He's also very observant of Wiley's ways.
Flexibility keeps things from breaking when pressure is applied the wrong way (or the right way for the wrong reasons!).

LASOs need to be nimble , quick, and flexible to adjust to changing operational needs and new technologies to meet those needs.

It is also helpful if the LASO is comfortable enough to understand the technologies involved at their agency; can interpret the policies so it can be properly applied to that technology, then be able to explain all that to their user community and management.

Not shown:
Politician – the ability to persuade, cajole, or otherwise influence others
Leader – or do it by example
Project Manager – The ability to keep track of multiple tasks and events at same time. Even if they are out of your direct control.
Meddler – In this case meddling is OK if something involves connectivity to KCJIS. So when someone tells you to "mind your own business", reply "I am!"

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

4. Ensure the approved and appropriate security measures are in place and working as expected.

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.

2. Identify and document how the equipment is connected to the state system.

3. Ensure that personnel security screening procedures are being followed as stated in this Policy.

6. The agency LASO is responsible for securing security awareness training and associated record keeping.

10

The FBI CJIS security policy lists 5 specific responsibilities “The LASO shall:” do.

KCJIS has added a 6th to also be responsible to ensure security awareness training is competed and records of it kept.

The numbers identify the order they appear in policy.

They are shown in the order we will discuss them in this course.

Use these resources to become familiar with all thing KCJIS.

Much of the KHP CJIS launch pad is fully accessible from any internet browser (although I.E. 11 is recommended) without any login required.
Other parts require your user ID (typically same as your KCJIS user ID) and a password in order to track your training progress or to protect information deemed sensitive.

The FBI CJIS Security Policy resource center is completely open to public access.
Feel free to share this with the contractors you use to support your network or software.

The KCJIS secure Web Portal currently requires a KCJIS userID and an RSA token for entry.
It has a bit of new look from previous years, but mostly the same functionality.
Informational materials regarding KCJIS systems, computer and network requirements , how to add new users, order tokens, etc. are located on this portal.

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

- KCJIS Policies and Procedures
  - KCJIS has adopted the FBI CJIS Security Policy as the foundational document for KCJIS policies.
  - Included as policy by reference are: Title 28 part 20, Code of Federal Regulations (CFR); The NCIC 2000 Operating Manual and associated Technical and Operational Updates (TOUs), The N-Dex Operations manual, and Kansas Statutes and Regulations.
- FBI CJIS Security Policy Version 5.5 6/1/2016
  - FBI Requirements and Tiering Document lists the 568 "shall" statements

In order to support policy compliance, you must know what the policies are.
Ignorance is not an excuse accepted by FBI auditors for out of compliance situations.

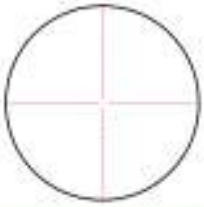
Resources exist for your edification regarding FBI CJIS and KCJIS security policies.

1. KCJIS has elected to use the FBI CJIS security policy format and language, then add our own requirements to further enhance KCJIS security.
   a. Beginning with version 5.4, KCJIS policy requirements are embedded within the FBI requirements.
      i. KCJIS policy either replaces (overwritten) a less restrictive FBI policy or
      ii. Is added to (before or after) FBI policies to further explain or bolster the policy.

2. The FBI authored a summary document of all "SHALL" statements contained in the FBI CSP.
   a. The "tier" assignment indicates whether the policy is
      (1) a MUST Prior to allowing access or
      (2) can be implemented post access.

   b. KCJIS version will be on the KHP CJIS Launch Pad > CJIS Documents > KCJIS POLICIES and COMMITTEE folder.

SCOPE



WHAT	UNENCRYPTED CJI	4.1 ; 5.10.1.2
WHERE	TRUSTED NETWORK(S)	5.10 ; 5.7 ; 5.13
	PHYSICALLY SECURE LOCATION	5.9 ; 5.8
WHO	AUTHORIZED PERSONNEL	5.12 ; 5.2 ; 5.1 ; 5.5 ; 5.6

13

As we go through some of the requirements remember:
FBI CJIS Security Policy and KCJIS Policies and Procedures are about protecting CJI.
While it covers all media and types of formats CJI can appear in, it's primary focus is digital data.

The easiest way to protect electronic data is to encrypt it.

So we most need to be concerned with UNENCRYTPED (think of it as "unprotected") CJI.
Where and how that unencrypted CJI is encountered, and by whom.

If you want to simplify your life as a LASO, keep these 3 considerations of scope in mind.

4 CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

4.1 Criminal Justice Information (CJI)

Criminal Justice Information is the ***term used to refer to all of the FBI CJIS and KCJIS provided data*** necessary for law enforcement and civil agencies to perform their missions …

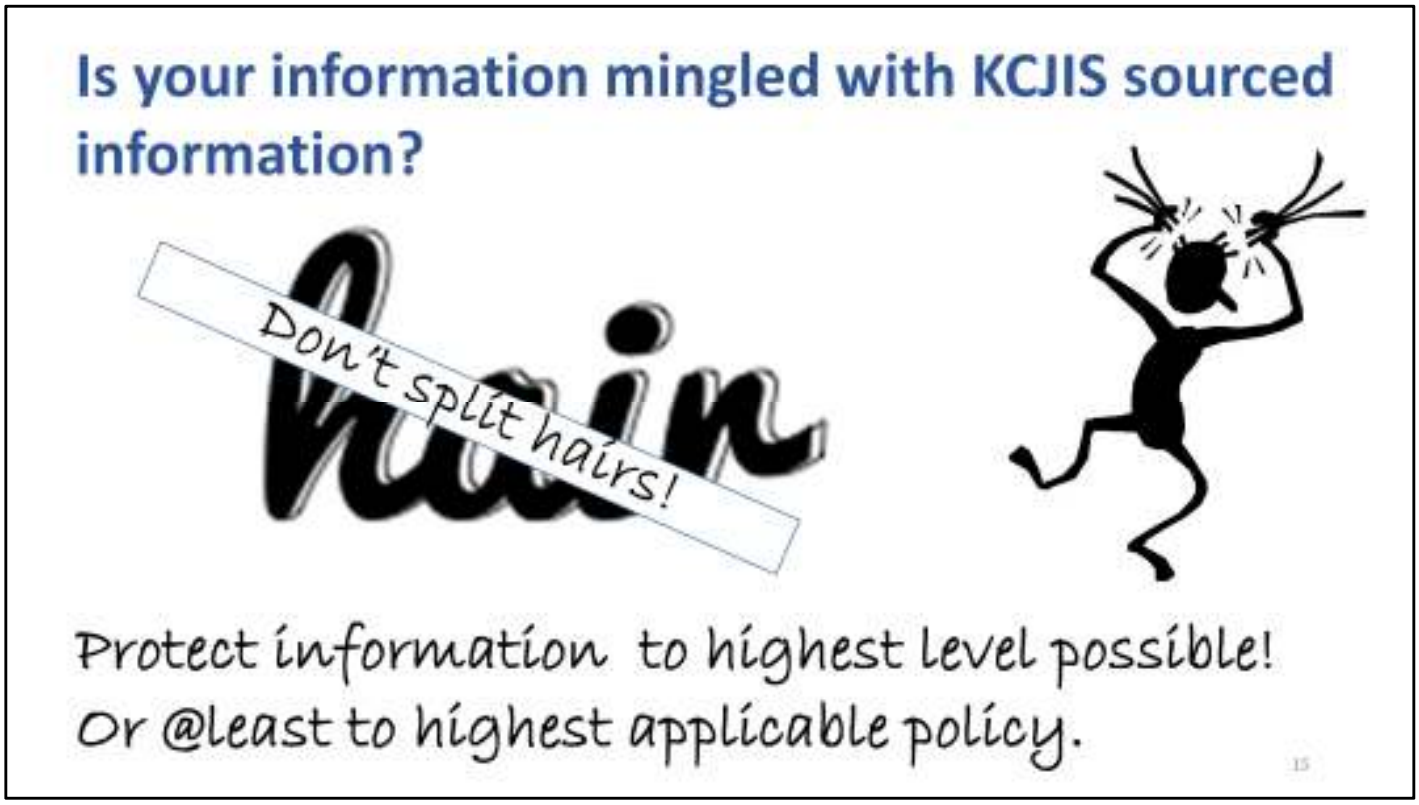
KCJIS POLICIES and AUDIT are applicable if:

The source of the information is KCJIS.
"As if you are borrowing".

In your job, you will encounter sensitive data. Some you collect yourself, some you ***have to get from KCJIS***. Policy is concerned with the information you have to get from KCJIS. The stuff you will not know any other way, like an event 12 years ago in Tucumcari, New Mexico that had an arrest, but no conviction. Consider that kind of data - obtained only because of KCJIS – as BORROWED. It belongs to someone else.
The analogy we've chosen here is borrowing your neighbors lawnmower. You received it in good condition and working exceptionally well. If you return it broken down, or you extend your loan of the mower to another neighbor without asking the owner… what do you think the odds are of the lending neighbor letting you borrow it (or anything else) ever again?

Information from another agency in Kansas, another state, or in some cases other countries, is kind of like that. You are allowed to use it for the benefit of your agency and your citizens – with strings attached. The data owner may have reservations or concerns about how it gets used. Privacy is a big concern in today's litigious society. Federal (title 28 CFR) and state (KSA 22-4701) laws attest to that.

Some things you get from KCJIS are meant to be given out to the public for the best interests of everyone – like road conditions or Amber alerts. Others can be given out in small pieces that limit the information to no real detail – like a driver's licenser photo that is just a picture of a person. (But TMI will get you into trouble!) Its all in policy area 4.



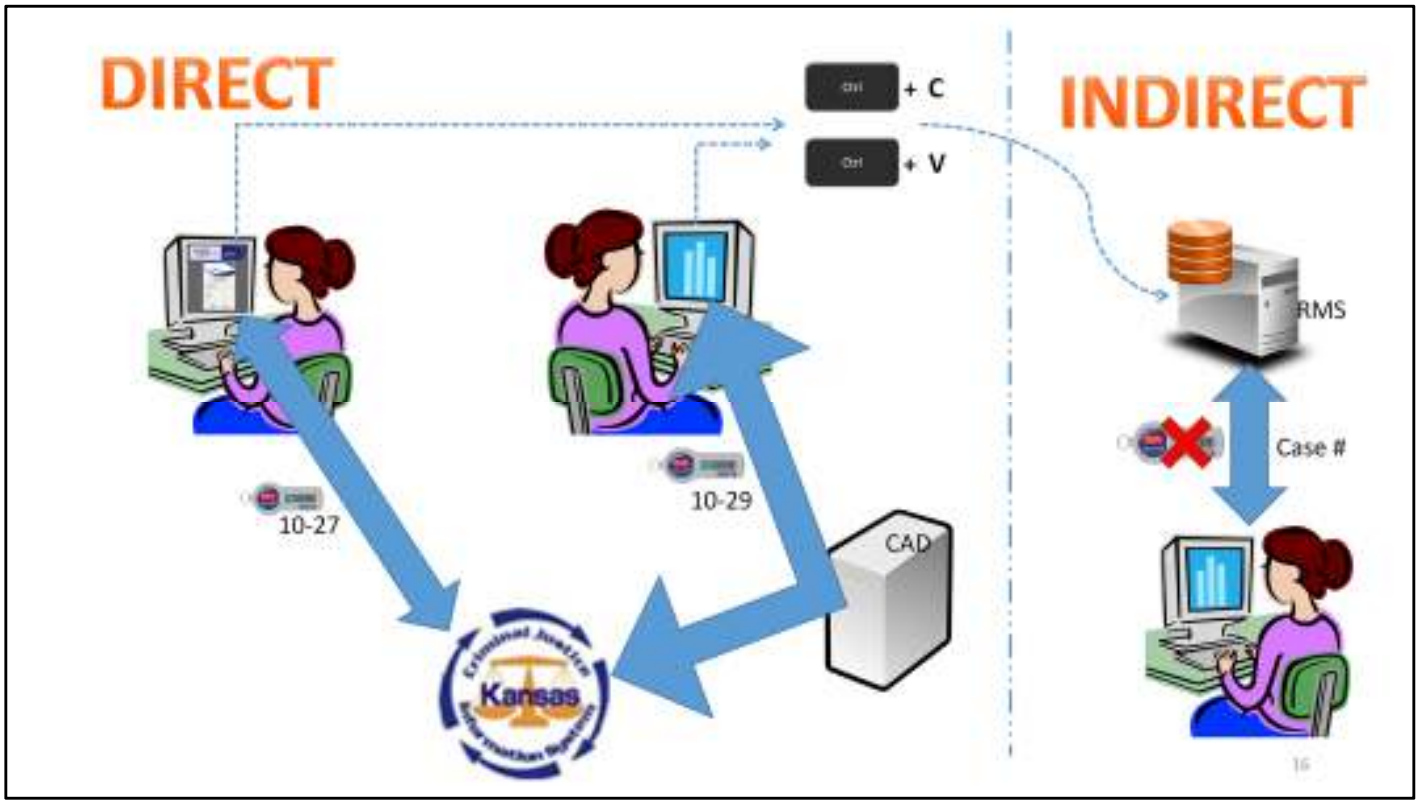
The Scope of WHERE is 2 faceted.

1. Where did you get the information from in the first place?

2. Where do you keep the information once you have it?

What happens when your investigation information is saved to the same case file as the information from KCJIS?
FBI and KCJIS POLICIES APPLY, that's what!

While the file is at rest in your systems, it all needs to be protected at KCJIS required level of security or better.
You may research ways to redact KCJIS obtained information when preparing something for dissemination.
You may discover that you will be money and time ahead to have agency dissemination policies that parallel KCJIS and FBI policies.



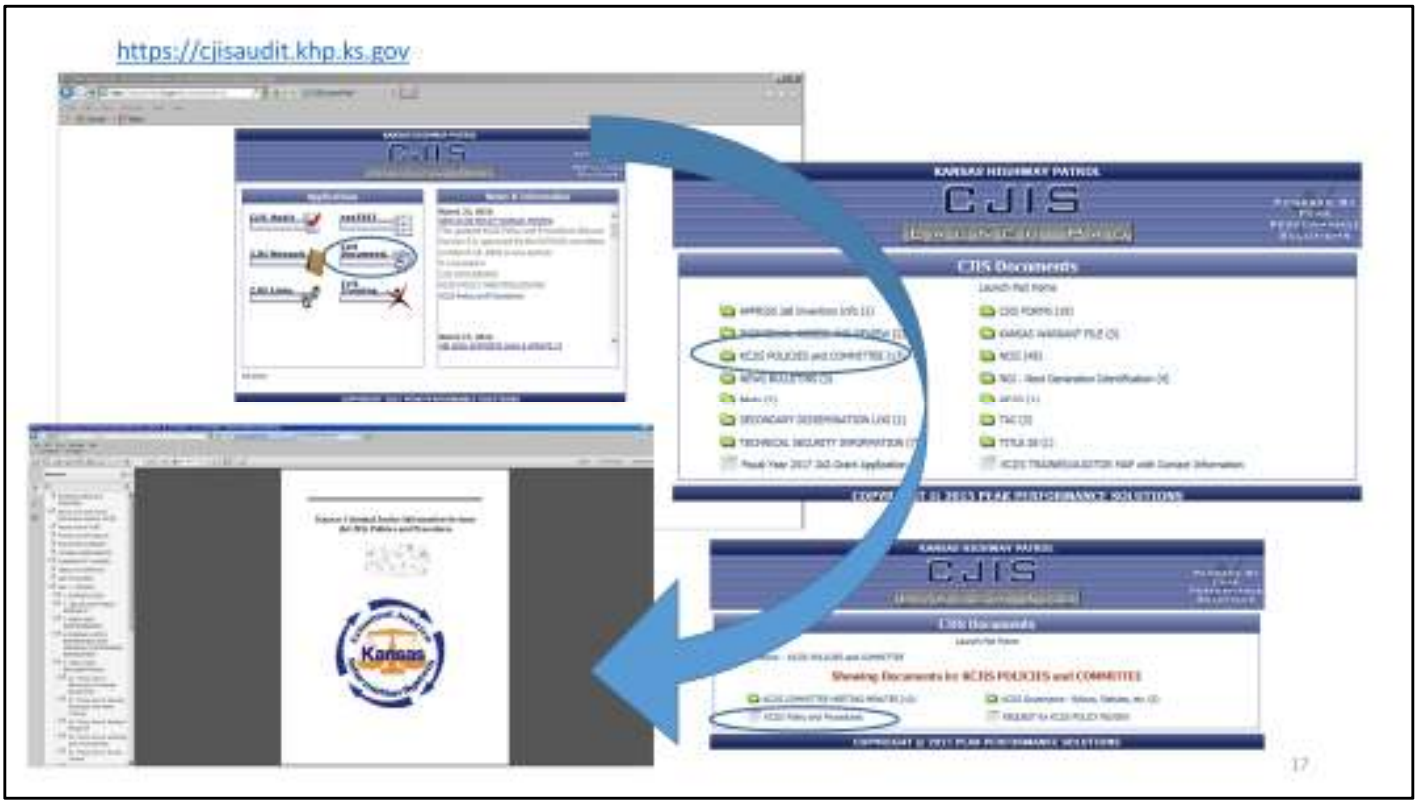
Another important thing to distinguish is the TYPE of ACCESS.

Direct Access — (1) **Having the authority to access systems managed by the FBI CJIS Division, *or KCJIS***, whether by manual or automated methods, **not requiring the assistance of, or intervention by, any other party or agency** (28 CFR, Chapter 1, Part 20). (2) **Having the authority to query or update** national databases maintained by the FBI CJIS Division, *or state databases provided by KCJIS,* including national *or state* queries and updates automatically or manually generated by the CSA *or KBI*.

Indirect Access – Having the authority to access systems containing CJI **without providing the user the ability to conduct transactional activities (the capability to query or update)** on state and national systems (e.g. CJIS Systems Agency (CSA), State Identification Bureau (SIB), or national repositories).

One agency person could have DIRECT ACCESS to query the NCIC person file. Then that person could populate a local agency case record in the RMS with that information.
A second agency person could then have INDIRECT access to the information that is now saved to the RMS. The information in your local RMS is historical. Someone would need to run new queries for absolute latest information.

Releasing information to others who did not login and make the query themselves - such as any printouts, fax, or any voice communication - is also INDIRECT ACCESS.



There are a few ways to access current KCJIS policies.
NOTE: The pdf file's appearance and features may be different depending on your browser, default pdf reader, and other application settings.

Public access – share easily with anyone who needs to know.

Go to https://cjisaudit.khp.ks.gov

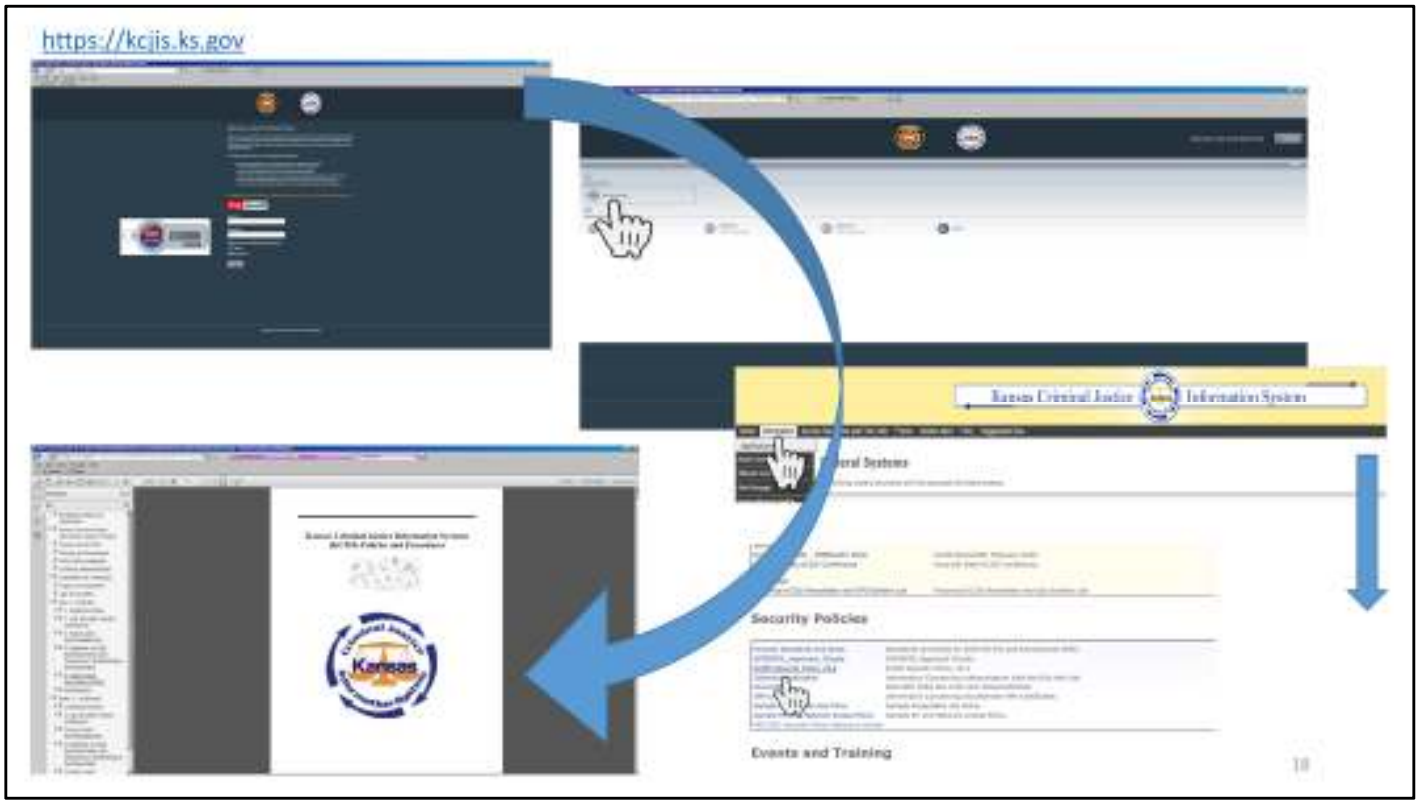
Click into the CJIS DOCUMENTS

Locate and open the KCJIS POLICIES and COMMITTEE folder

Click KCJIS Policy and Procedures

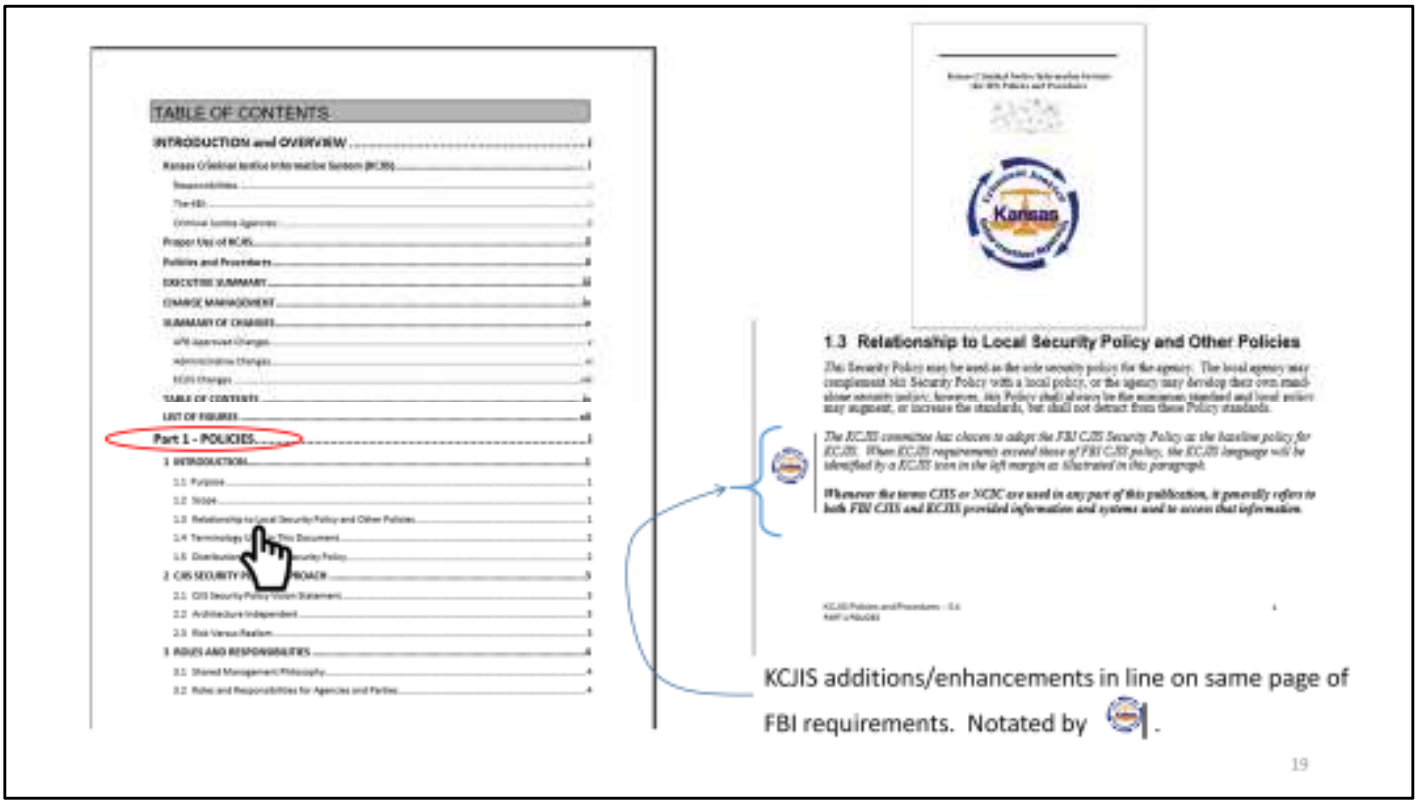
The manual will open in your browser.

Also from the launch pad, but not shown, you may access the manual from CJIS Manuals.
When entering CJIS Manuals, you will be prompted for your NexTEST username and password.
Once in, select KCJIS Policy & Procedures.
The Manual will open as a single chapter.



If you have a KCJIS token and use the KCJIS Web Portal, you may also access the manual there.

Once authenticated…
Click KCJIS Portal
From the Portal Menu Bar, select Information
SCROLL DOWN to Security Policies
Locate and click to open KCJIS Security Policy v5.x

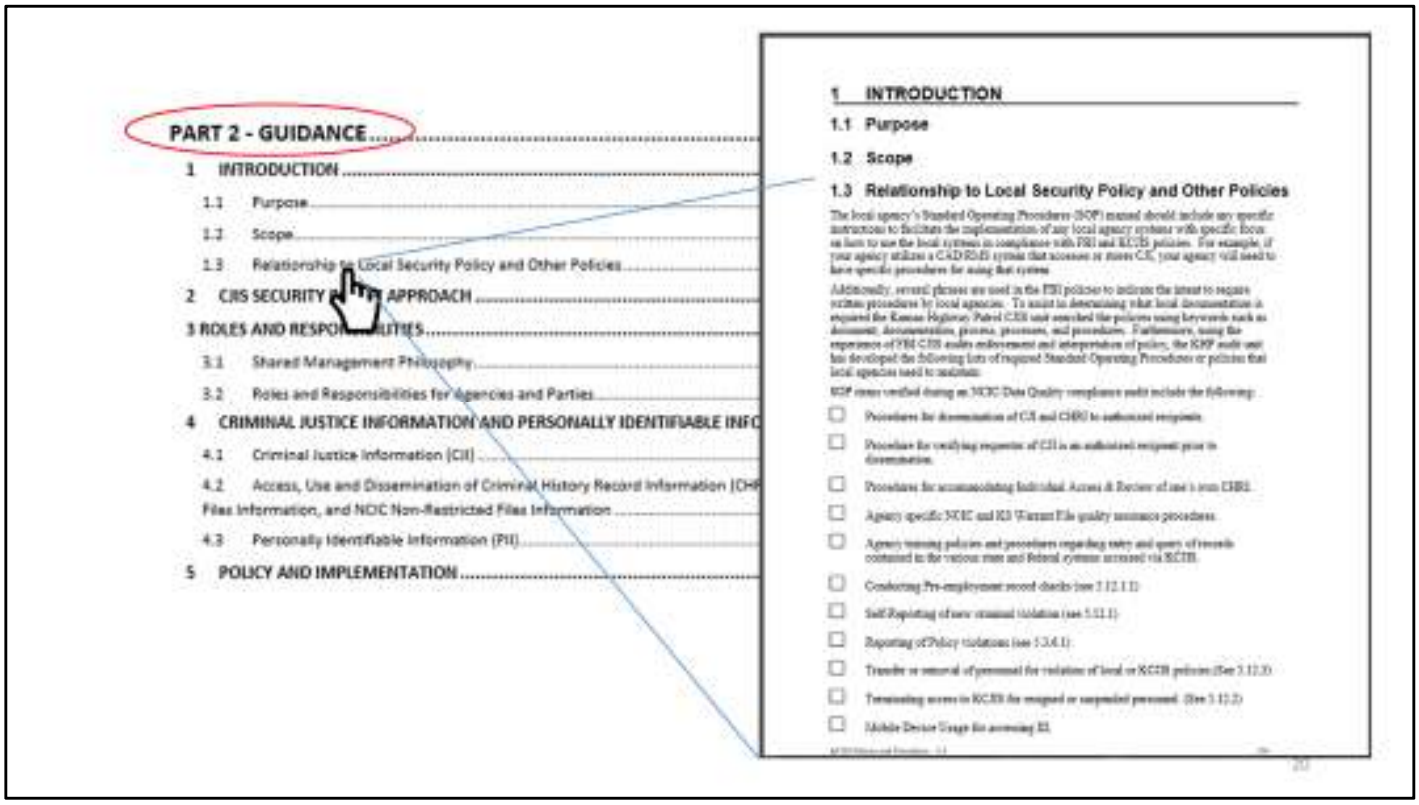


Once you have located and opened the policy manual…

The Table of Contents is linked to the represented text within the body of the KCJIS manual. You may also use the Bookmark feature of the Adobe reader (depending on version) to access specific policies.

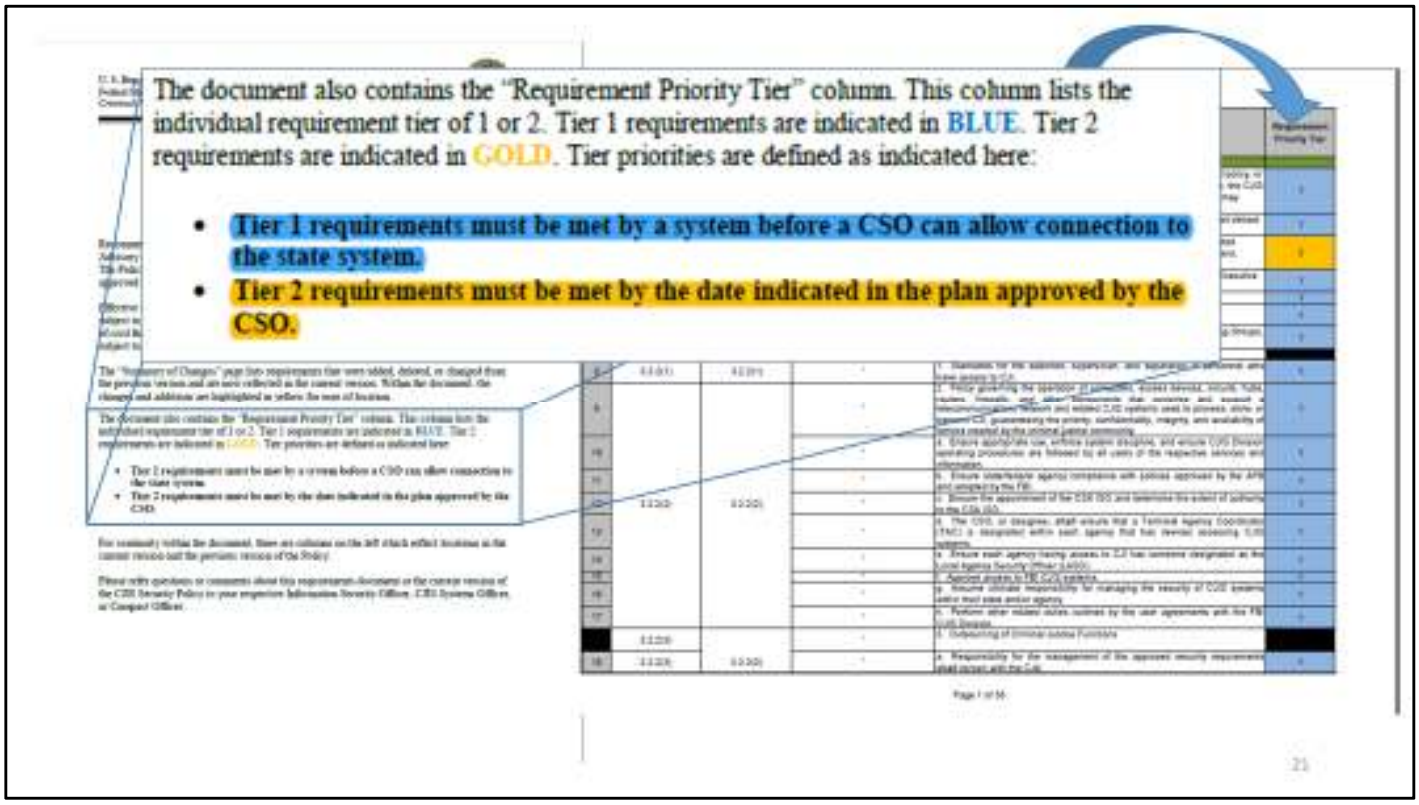
Part 1 of the manual are the policies.
They are what the KHP technical security auditors will be looking for.

As illustrated here, the KCJIS logo, a vertical line and *italicized text* call your attention to when KCJIS has imposed a stricter or additional policy.



Now, Part 2 of the KCJIS manual is intended as guidance.

A much shorter “chapter”, it only contains items where explanations or other helpful information can help your agency to comply with the requirements in Part 1.



The FBI has enhanced their Requirements Document to now include a column for "Requirement Priority Tier".

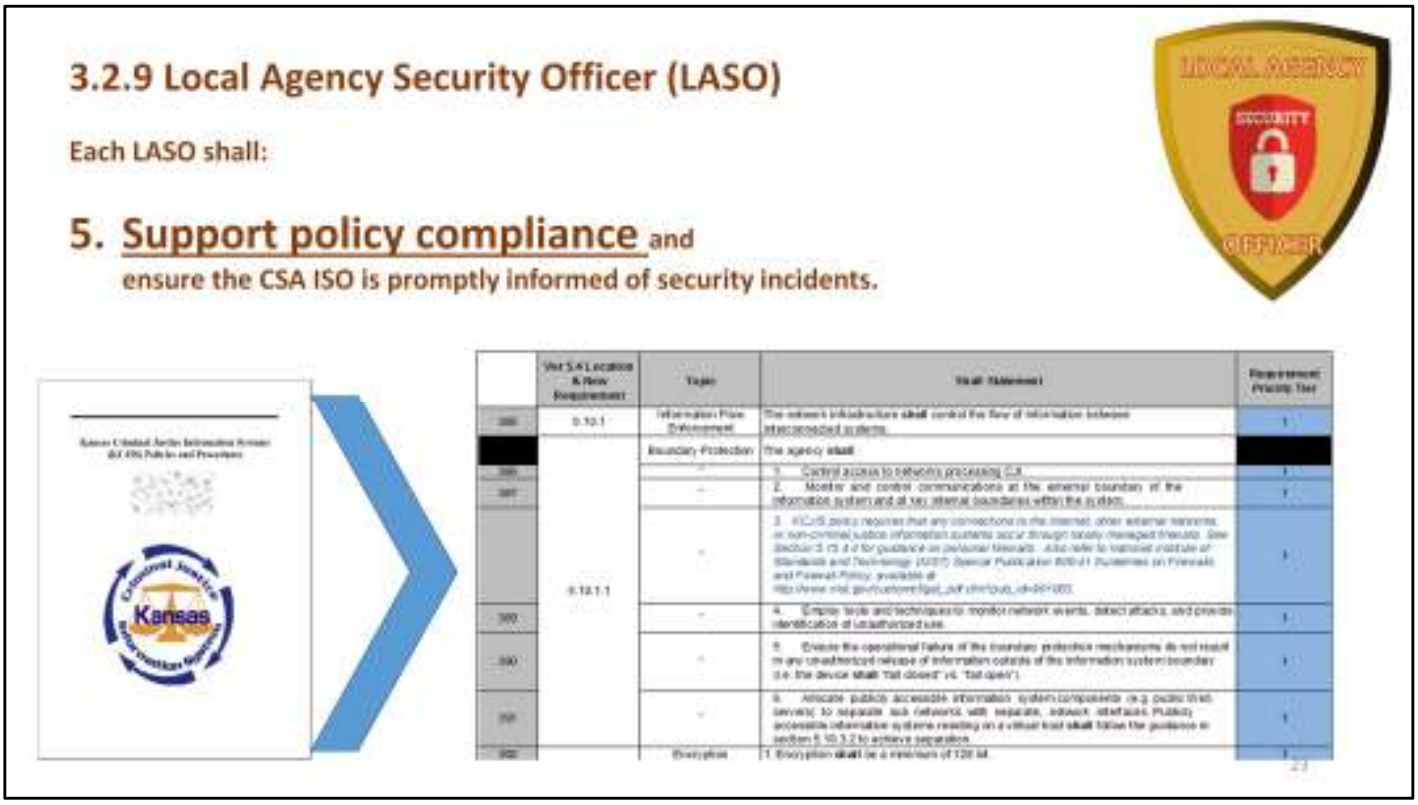
MOST requirements, indicated by the shall statements, must be in place PRIOR to new approvals.
Some can be slipped in when there is a plan and time frame.

As already mentioned, KCJIS has elected to use the FBI CJIS security policy format and language, then add our own requirements to further enhance KCJIS security.

So, we have also edited the FBI Requirements Document that lists all the “SHALL” statements to include KCJIS requirements, too.

It can be found on the KHP CJIS Launch Pad.
CJIS DOCUMENTS
KCJIS POLICIES and COMMITTEE folder
(same folder as the policy itself).

In this illustrated example, KCJIS has ADDED requirements to FBI CSP.
(LASO Shall #6 and notification requirement are KCJIS specific.)
KCJIS additions are presented in the order of its location within the actual policy.



In policy area 5.10.1.1, KCJIS *superseded* the FBI's sub #3 by replacing the FBI's requirement with specifics that any external network connections be made through a locally managed firewall.

Notice that we have tried to call attention when KCJIS exceeds FBI policy by changing the font to *blue italicized*.

3.2.9 Local Agency Security Officer (LASO)

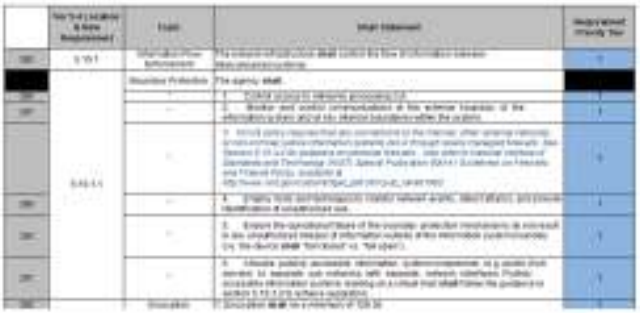
Each LASO shall:

5. **Support policy compliance** and ensure the CSA ISO is promptly informed of security incidents.

5.11 Policy Area 11: Formal Audits

5.11.2.2 Triennial Security Audits by the Kansas Highway Patrol CJIS Unit

- Based on KCJIS Policies and Procedures
  - FBI CSP
  - KCJIS additions
  - Requirements and Tiering Document lists the "shall" statements.
- Your Information Technology Security Auditor will contact you "when it's time".
- Complete the questionnaire your auditor will provide.
  - On site will go quicker
- On site visit to confirm physical security and hardware.
- Excellent time for 1 to 1 training and questions answered.



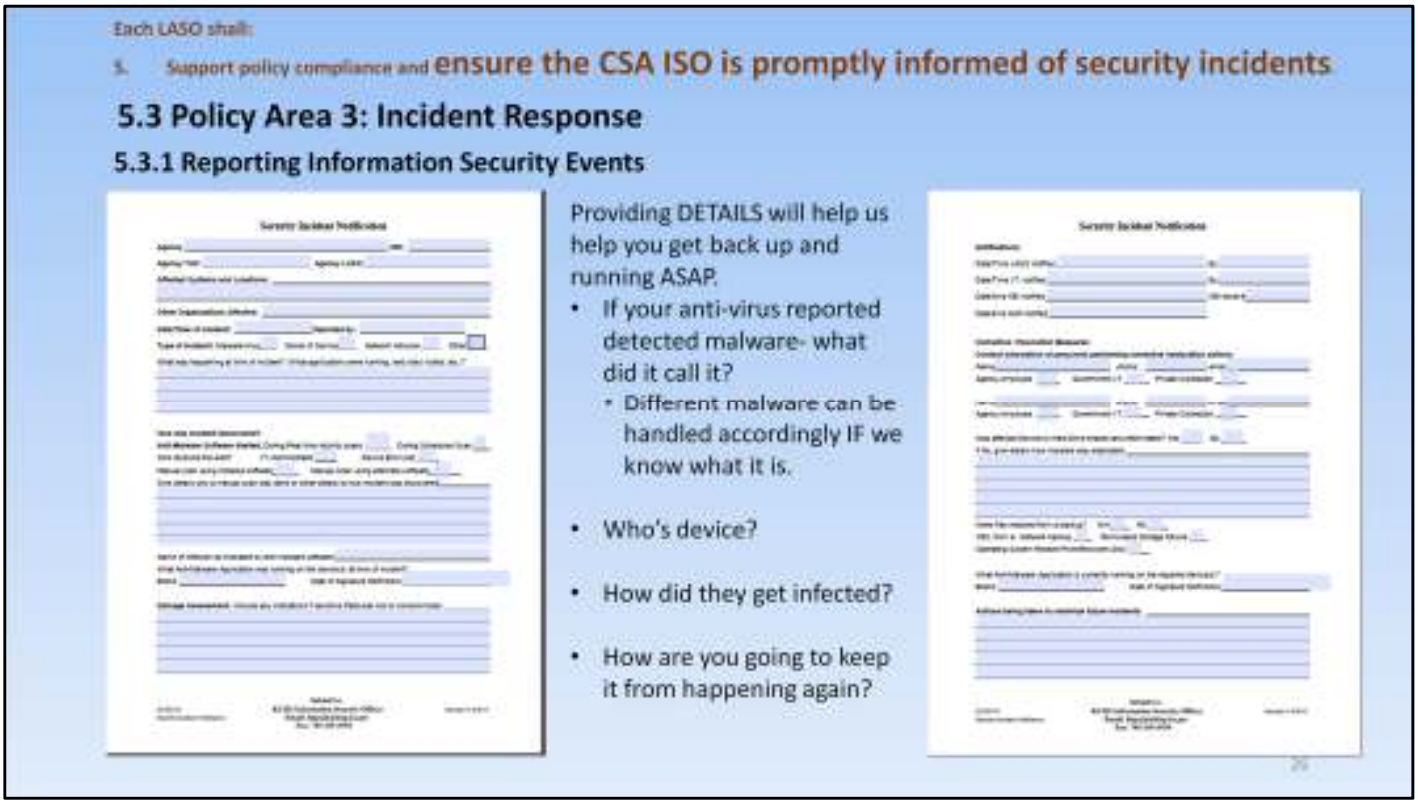
Every 3 years, the FBI CJIS Audit Unit visits Kansas to see how well the KHP (as CSA) and KBI (as SIB) are doing on spreading the word and applying the FBI CJIS security policies to KCJIS.

So, the KHP CJIS Unit has an Information Technology Security Audit staff that audit local agencies (you) every 3 years, too.

Historically, the FBI has audited against the entire FBI CJIS security policy, with no particular "points of emphasis", so that is what the KHP information technology security auditors do.

The KHP enhanced Requirements Document **IS THE INFORMATION TECHNOLOGY SECURITY AUDIT STANDARD**.

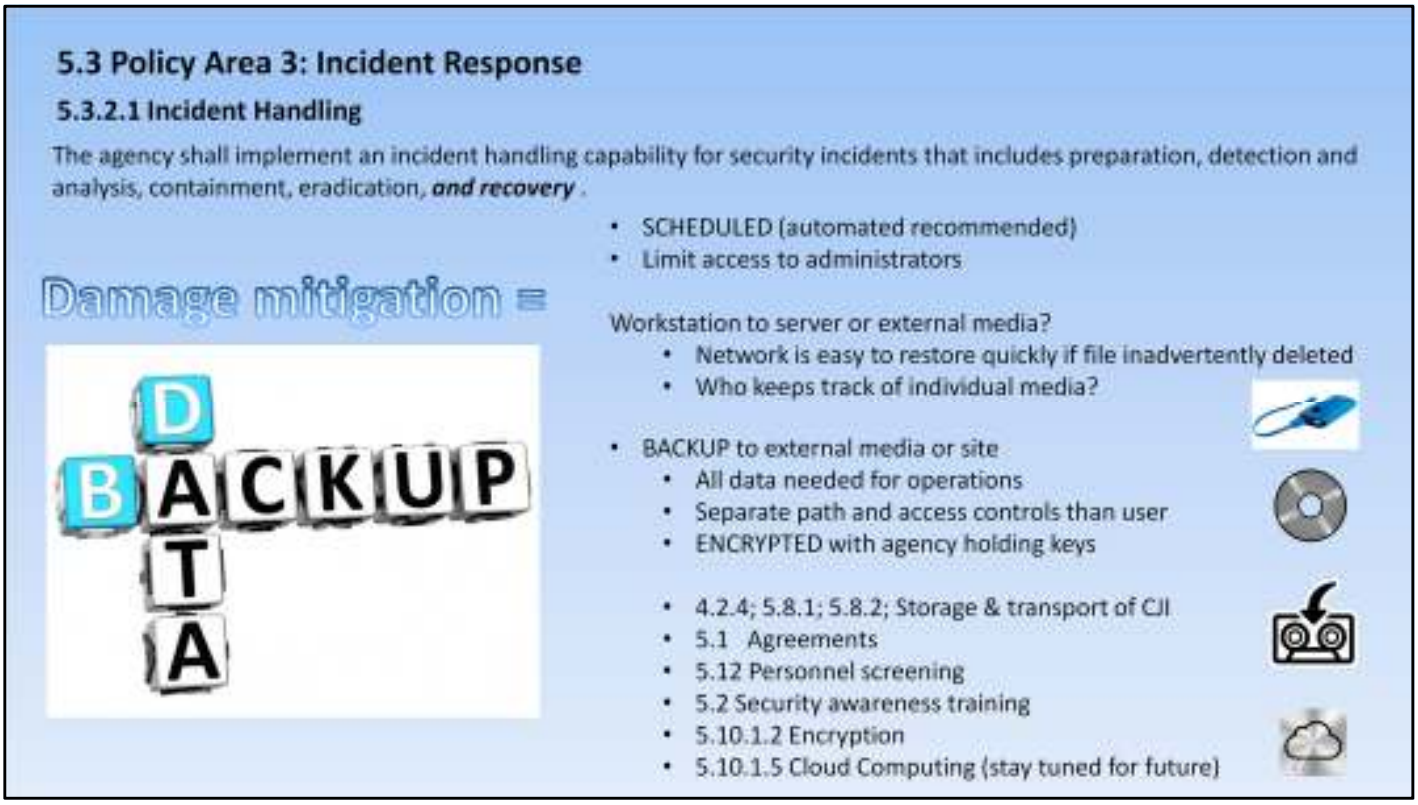
The FBI also created and made available to KHP an audit questionnaire. The KHP has modified that questionnaire to include KCJIS specifics.
We use that to conduct our audits.



Cyber attacks on systems containing CJI will continue.

They occur in various ways. Most are not targeting your agency. But they might! KCJIS needs to know if something or someone is trying to attack KCJIS or FBI CJIS systems through your devices.

The KCJIS 139 form is designed to give us answers to determine if there is more to the malware that we need to know, or if we need to take additional action to protect all of KCJIS.



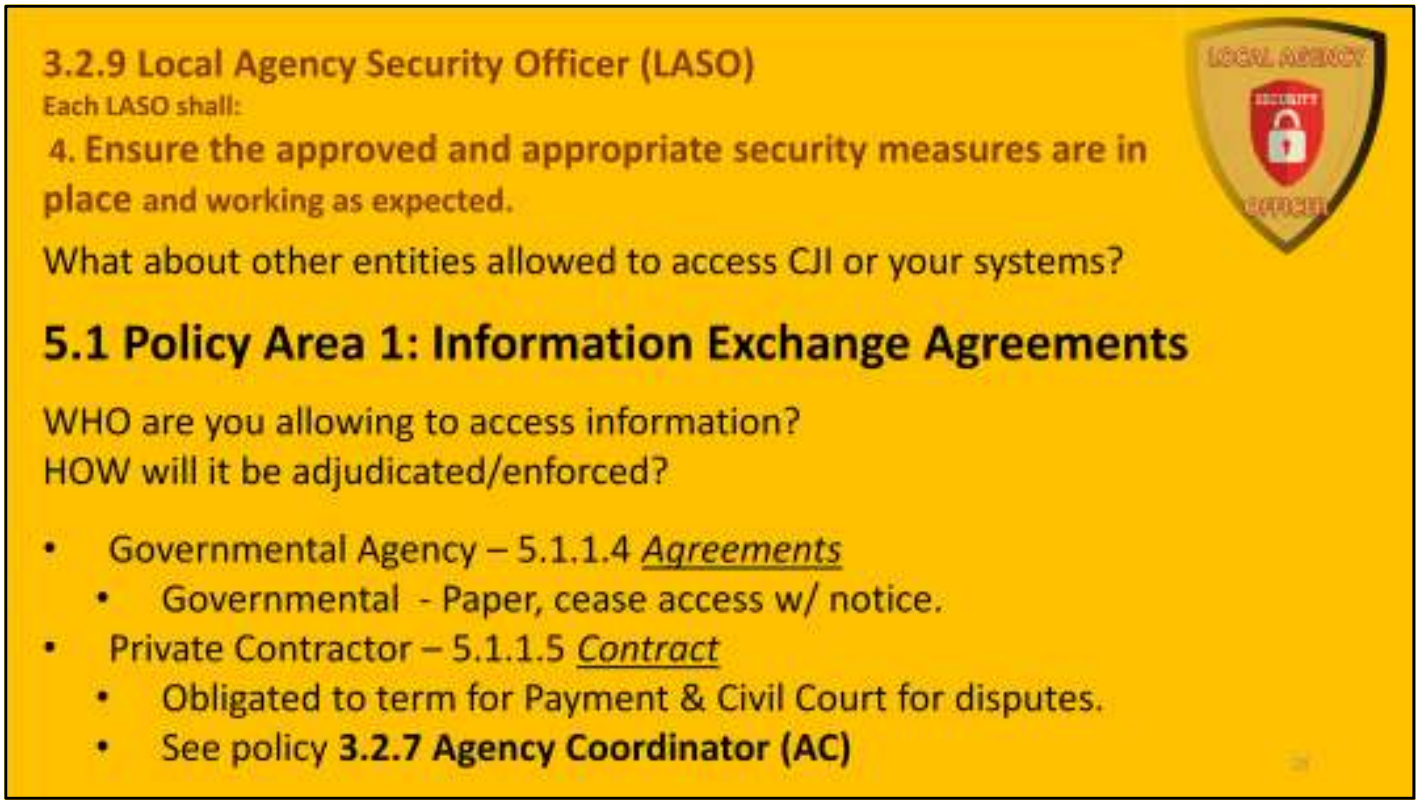
Backups ensure future availability of YOUR data should anything destructive happen.

- Natural (fire, flood, tornado)
- Mechanical failure (hard drive crash)
- Operator error (accidental deletion of file(s))
- Malcontent/ cybercrime.

The biggest craze in cybercrime lately appears to be ransomware.
Ransomware, as the name implies, is malware that encrypts YOUR data rendering it inaccessible to you.
Then the crooks demand a ransom from you to get it back.
This has proven to be VERY lucrative because users don't have backups!

FOIL the bad guys!
Back it up BEFORE they get to it.
No ransom needs to be paid!
If everyone did this, there would be no ransomware.

Refer to the policies listed on the slide when you develop a plan and resources (personnel) to carry it out within KCJIS compliance.

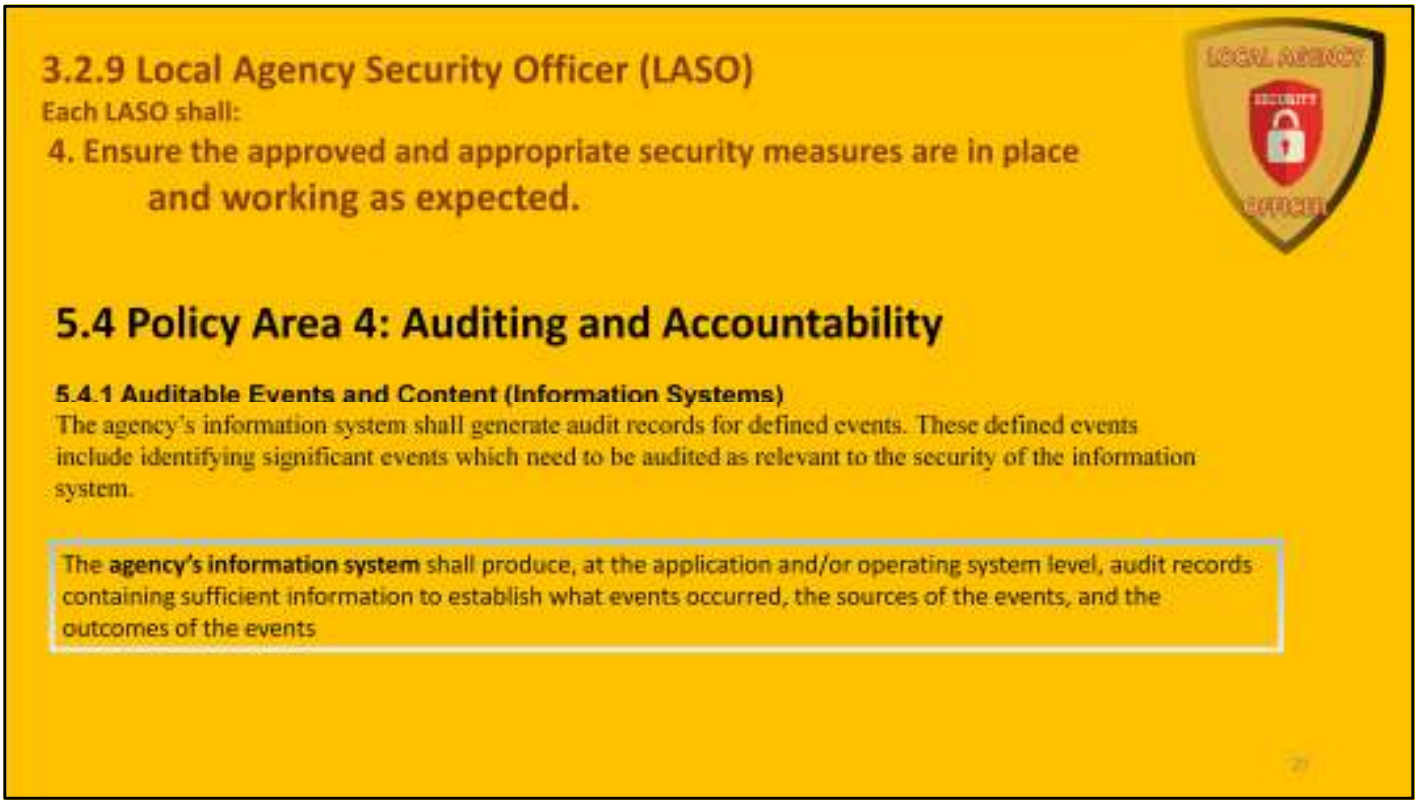


It is the LASOs responsibility to ensure the working measures are in place. That will require you to "keep your ear to the ground" and to be actively involved in the operation of current systems as well as the design of potential new ones. In other words - be an involved part of the team.

When sharing CJI, it is important that everyone involved know their responsibilities.
That is where the written information exchange agreements come in.
Use the requirements of area 5.1 to make clear who has what responsibilities among all the parties. And, address contingencies in the event one or more parties cannot fulfill their obligation.

Different personnel and relationships to the agency require different agreements.
AGREEMENTS and CONTRACTS both provide for the clarity of responsibilities, limitation of uses, etc. The difference is how it can be enforced.
Or perhaps better is Who adjudicates any questions or disputes.

Agreements = Just between the parties to start.
Contract = Money (payment/non-payment for services) is involved.
Committed to specified time frames
– for completion of projects or length of agreement.
A court of law may have to decide any contested issues.



Policy area 5.4 involves how to ensure security measures are in place. This auditing is NOT a person coming to inspect your network and ask questions (that's area 5.11). Rather is concerned with audit trails in your system(s). Ask your technology providers how to tell the who, what, and when of both successful and unsuccessful attempts to access CJI systems. If you ever worked in retail stores and ran the cash registers you may be familiar with "detail tapes". They were the second printed tape produced by the cash register (of yesteryear anyway) that showed the details of every transaction: The operator, day and time, items they "rang up", how the customer paid, how much change was due back, etc. These details of "what happened" can be reviewed by management to determine if an employee is prone to mistakes or being dishonest. Policy area 5.4 is calling for a similar level of detail be kept regarding access to systems processing CJI.

Regular review of this information can indicate when things aren't right. They may also verify that the controls are working.
KCJIS logs activity that occurs via the Central message Switch, but KCJIS does NOT have access to log what activity occurs on your OWN systems.
Furthermore, your operating system may log access into your network, computer, hard drives or network storage and possibly even access of an application. But the OS can't detect all activities within any specific application.

In the most recent (2014) FBI technical audit, some agency's CAD/RMS systems were identified that did not log the prescribed events occurring within those systems.

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.

- 5.5 Policy Area 5: Access Control
- 5.6 Policy Area 6: Identification and Authentication
  - KACIS

    COMING - SPRING 2017
    Identity and Access Management
  - OpenFox Configurator

31

Area 5.5 Access Controls can be **physical access** by keeping doors to certain areas shut and locked (including police vehicles – see 5.9) Old fashioned keys work!
Electronic key cards or other managed access tools not only control who can access but when, and can provide nice details as to who came or went and when.

Some **systems** can control access by the who, when, and even the "from where". They include: Access Control Lists (ACLs) or other rules on network infrastructure appliances like firewalls and routers. Directory services such as Microsoft's Active Directory on network servers that control user access through policies and group memberships.

Area 5.6 is about individuals making a claim (assertion) of who they are, then presenting proper credentials to prove the assertion.
Users accessing your systems need to be uniquely identified and not share a generic username.
Authentication factors are the credentials. The "something you know" , "something you have", or "something you are".
A typical single factor authentication uses a password ("something you know") to verify the identity assertion.
Multi factor authentication requires 2 or more ways from different authentication types to verify an identity like digital smart cards ("something you have") or fingerprints or retina scans ("something you are").
KCJIS currently uses a PIN (something you know) and an RSA SecureID token (something you have).

KACIS is the current administration tool for all KCJIS user access. Stay tuned for news on KBI initiatives!
OpenFox configurator is used to set message key access to state, NCIC and Nlets files by user.

KCJIS access currently begins with KACIS.
Then for message switch (NCIC access) TAC needs OpenFox Configurator.
KCJIS Web Portal for ordering extra tokens, etc.

KBI is working on a NEW Identification and Access Management solution that is likely to change KACIS usage.

- ETA: 1st quarter 2017

- Will have some workflow processes that will eliminate some KCJIS forms.
- Later phases may be able to replace RSA tokens
    - Be careful what you ask for!
    - 5.6.2.2 Advanced Authentication may become an agency responsibility option.

- Bottom Line: Keep KCJIS (KHP ITSA) in loop as you move toward any NEW systems.
    - We'll keep you in touch with KBI to ensure future compatibility.

5.12.2 Personnel Termination
The agency, upon termination of individual employment, shall immediately terminate access to CJI.

5.5.1 Account Management
... The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.

System accounts of personnel who are no longer active for any reason may be used maliciously.

Accounts should be deactivated when a person will be away from work for extended periods.
- Active Duty military deployment
- Family medical leave

In additional when someone leaves permanently, their accounts and credentials should be disabled.
- Retirement
- Death
- Fired
- Relocation

Upon personnel transfers, account's need to be reviewed and access to information removed or added based on their new assignment.
- LEO to civilian position
- Civilian turns LEO
- Dispatcher moves to corrections officer
- Etc.

Access reviews can be done at time of annual record checks.

In the most recent (2014) FBI technical audit, password policy was out of compliance at some agencies because passwords at neither their Operating Systems (Windows) or their CAD /RMS systems met one or more of the following requirements:

- Minimum of 8 characters
- Must expire within at least 90 days
- Passwords can not be reused more frequently than the 10 minimum in policy
  (1st password can be re-used on the 11th change)

Be sure your SYSTEMS can enforce the minimum requirements (or better).
They can be at Operating Systems and/or Application levels.
But they have to be somewhere before accessing CJI.

5.6 Policy Area 6: Identification and Authentication

5.6.2.1 Standard Authenticators

5.6.2.1.2 Personal Identification Number (PIN)

When agencies utilize a PIN in conjunction with a certificate or **a token** (e.g. key fob with rolling numbers) **for the purpose of advanced authentication**, agencies shall follow the PIN attributes described below

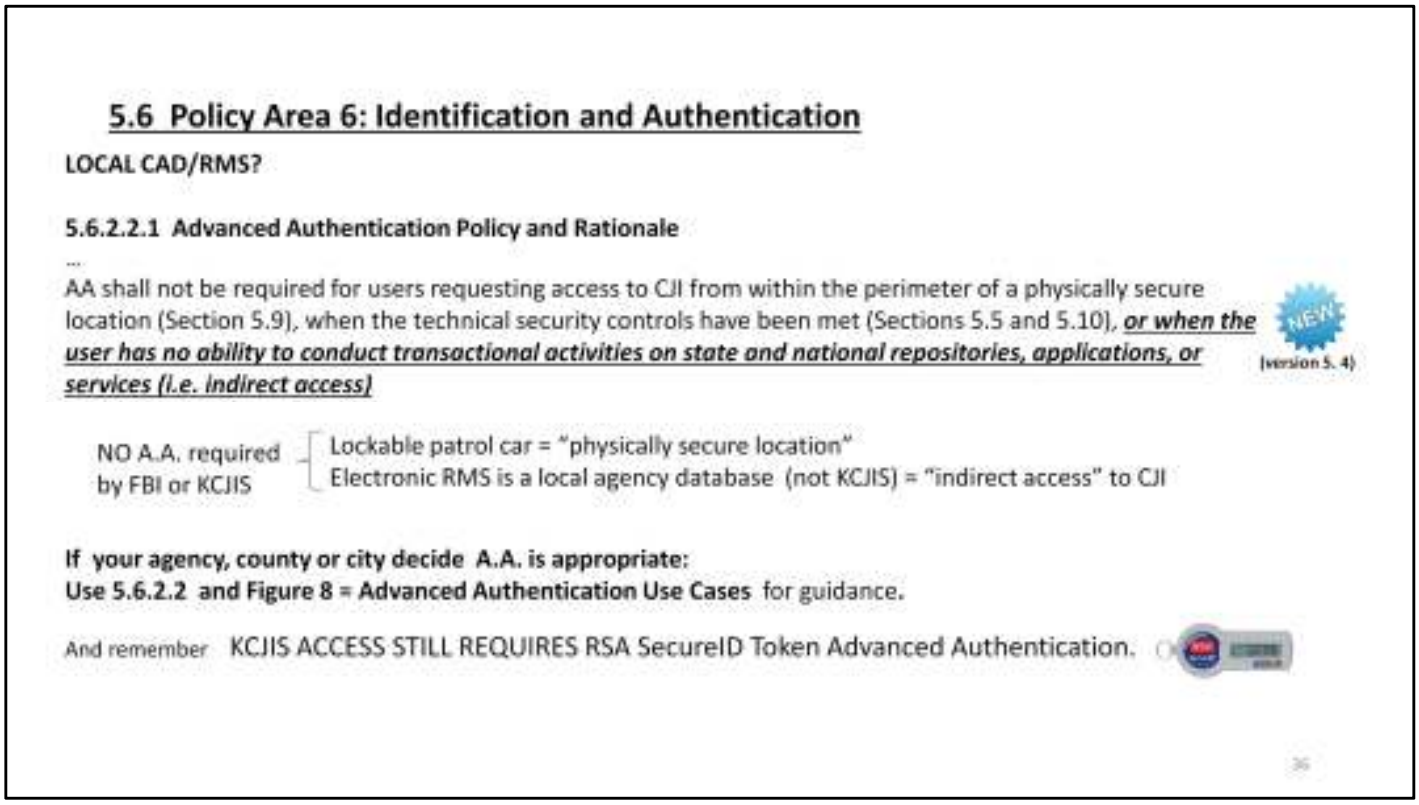
1. **Be a minimum of six (6) digits**
2. Have no repeating digits (i.e., 112233)
3. Have no sequential patterns (i.e., 123456)
4. Not be the same as the Userid.
5. **Expire within a maximum of 365 calendar days.**
6. Not be identical to the previous three (3) PINs.
7. Not be transmitted in the clear outside the secure location.
8. Not be displayed when entered.

Related to passwords are our PINs.
The newer PIN policy will affect your KCJIS user login.

If your CAD accesses KCJIS, is it setup to allow at least 6 digits for your PIN?

New users should be setup with 6 - 8.
KCJIS is currently in a transition period for us older folk that had as short as 4.
BUT, the day of reckoning will come!

You may reset your PIN anytime. By contacting KBI helpdesk 785-296-8245.
(Just don't all call at once).



Advance Authentication is no longer required by FBI or KCJIS policies ***to access your own databases***. Even if it contains information obtained solely by way of KCJIS.
So, **KCJIS users need a token**. Non-KCJIS users don't (if your agency decides to implement their own AA solution, they should consult with the KBI Security Office prior to purchase to facilitate the possibility of using your solution for future "federated" KCJIS access).

Example:
A.A. in the form of KCJIS User ID + PIN (something they know) + RSA TOKEN (something they have) - is STILL REQURED FOR KCJIS –
was used by a user for their DIRECT Access to KCJIS to obtain the information.

They subsequently saved the information to the local agency RMS.

Now, the local database (RMS) contains a historical record that may not reflect current information in the NCIC or Kansas CCH record.

Next, a user (same or different) enters their local agency userid + password to access (INDIRECTLY) the CJI contained in the RMS.
This user has NOT accessed KCJIS or NCIC so they cannot affect any changes to the subjects current record contained "upstream" in state or national systems.
Policy allows for this. The burden of protection is on the agency, not KCJIS.

5.6 Policy Area 6: Identification and Authentication

LOCAL CAD/RMS?

5.6.2.2.1 Advanced Authentication Policy and Rationale

2 Case studies of a patrol officer with an MDT in their patrol car.

1. Officer runs own 27, 28, etc.
   a. Unique username + password for MDT/agency resources
   b. KCJIS User ID + PIN + TOKEN still required to access anything at or through KCJIS.

2. Officer only receives dispatches and enters information such as arrival time, narratives, and information obtained on scene.
   a. Unique username + password for MDT/agency resources

37

2 Case studies of a patrol officer with an MDT in their patrol car.

A unique Userid and robust password to authenticate to the MDT and agency systems is required in BOTH cases.

Case #1: They use it to receive dispatch messages from their 911 center, AND have the ability to run their own queries against Kansas and NCIC files. Assuming proper approvals have been made via KHP for the device… The officer will also need to have a KCJIS user ID assigned and an RSA token to access the Kansas message switch to run their own queries.

Case #2: They use it only to receive new dispatch messages from their communication center. Since NO KCJIS access is done, no RSA token is required by KCJIS.

Careful: BOTH cases will require encryption of CJI

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

2. Identify and document how the equipment is connected to the state system.

5.7 Policy Area 7: Configuration Management

5.7.1.2 Network Diagram

- ❑ CURRENT
- ❑ Shows interconnectivity and separation of CJA from NCJA
- ❑ "For Official Use Only " to mitigate KORA, etc.

- ❑ KCJIS 129 Network change request PACKET

It's a good idea for LASOs to take and maintain an inventory of KCJIS access devices. Your information technology security auditor can assist you in providing a report via OpenFox.

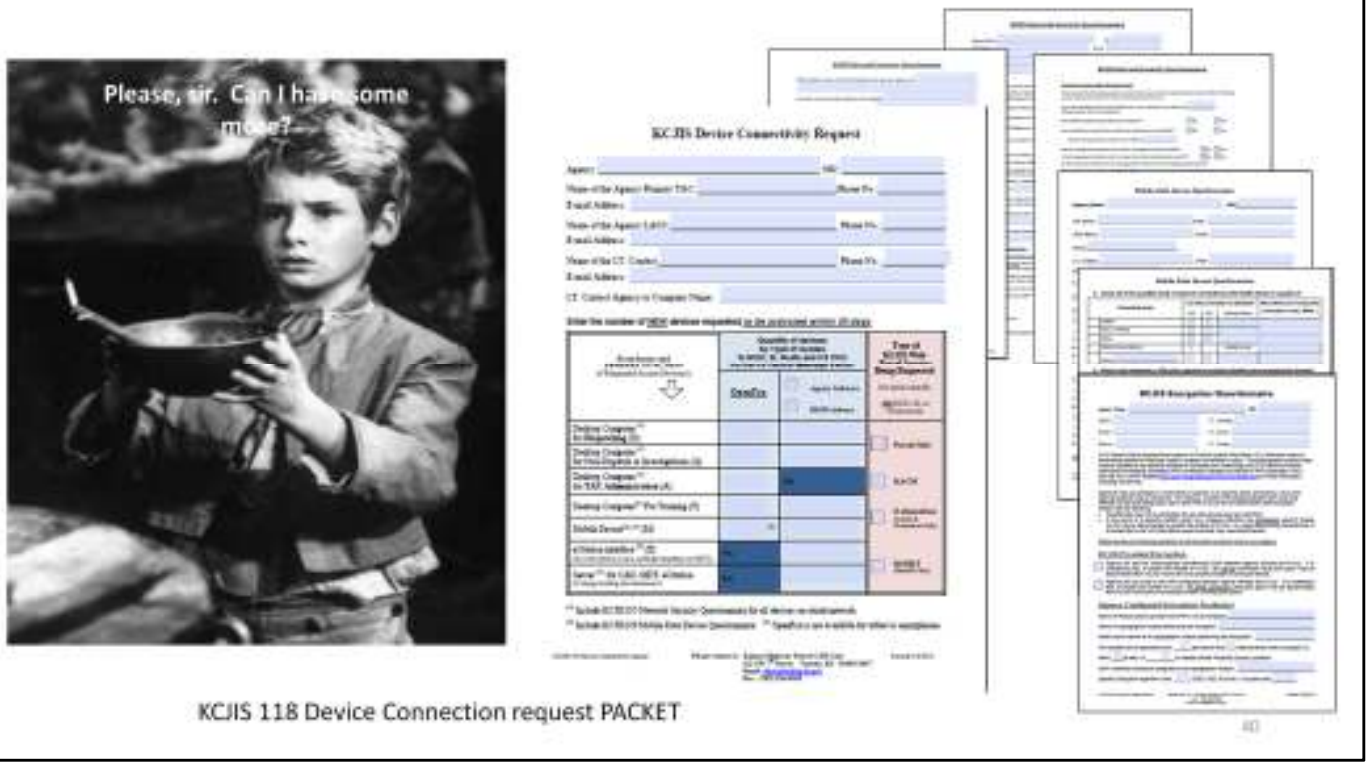
LASOs also need to know firewall(s) make & model. Time is saved when the LASO is aware and don't have to ask I.T. for this needed information requesting changes or new stuff.

Diagrams need to represent the general concept (high altitude overview – not every device) of where devices are on a wired network, and how CJI is kept apart from Non-Criminal Justice (city or county departments) stuff. Use the K.I.S.S. method of drawing and watch out for the TMI (Two Much Information) factor. You can represent a forest with a single tree. Like a road map, no specific addresses need to be included (in case the map gets into the wrong hands). No fancy software needed to draw diagram when Word text boxes and shapes work well. Appendix C is FBI samples.

Need to make a change? Let us review for compliance BEFORE you commit $$$.

Use KCJIS 129 for any changes.

- Changing VPN connection to KCJIS (from SecuRemote to Firewall site to site)
- Adding wireless access
- Moving to virtualized data center
- Physical relocation
- Etc.



Like the 129, the KCJIS 118 PACKET tries to gather all needed information for review in one place.
Has it been a while since you asked for more?
Many of same questions in network change.

Complete as much as you can. Ask I.T. for help.

Enter only quantities for New ADDTIONAL devices.

By the Way…

- Policy 5.10.1.3 requires Intrusion Detection
- Remember that if manufacturer no longer supports device or operating system, it is NON COMPLIANT

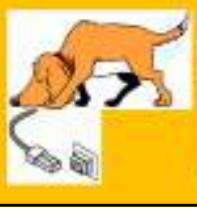
3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

3. Ensure that personnel security screening procedures are being followed as stated in this Policy.

5.12 Policy Area 12: Personnel Security

- Within 30 days for government employee assignment with DIRECT ACCESS to CJI systems.
- BEFORE contractor employee is granted ANY ACCESS to unencrypted (plaintext) CJI.
- Anyone with "roamin' around" access to areas where CJI is processed or stored.
- Anyone with unmonitored access to networks used to transmit unencrypted CJI.

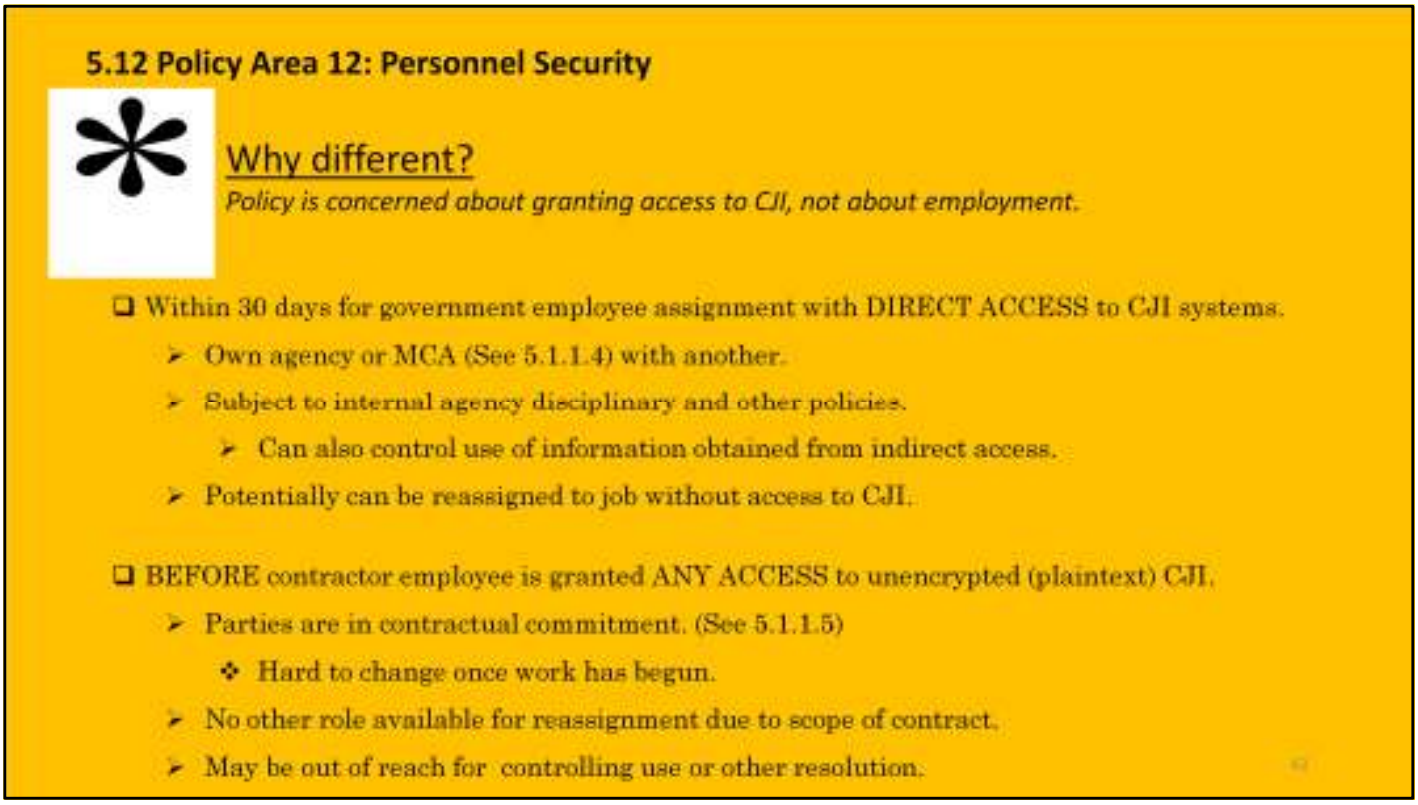



People make everything in any organization work (or not).
The best security equipment made will fail if the actions of someone inside the protective boundary circumvent security measures.
Personnel screening and security awareness training requirements tend to get lumped together because of the generalization of who is required to have them done.
However, there are some subtle differences. The point for this part of the course is that the LASO is called out in policy to be responsible to ensure these 2 tasks are being completed.

ANYONE who is UNESCORTED in a physically secure location must be properly record checked.

Don't want to hassle with checking everyone that roams your buildings? Reduce the "threat vector" by:

- Designate certain areas of the building as restricted access with signs and physical barriers (walls, counters, etc. see 5.9).
    - Allow only authorized personnel (by way of record checks and security awareness training) to access those areas.
- Leave any unattended network jacks unplugged in the wiring closets.
- Keep wiring closets and server rooms locked at all times with access by as few as needed.
- Escort - 100 % of the time - anyone who has not undergone proper record checks. Escort implies the ability to physically manage their access - not just observe on camera.



If they are an employee, they have 30 days (although we recommend completing the check prior to formal job offer). Grace period is allowed because of their relationship as an employee. If they are found to have disqualifiers, they can be reassigned to other jobs that don't have access to CJI or be subject to other agency policy for dismissal, etc.

Contractors, by the nature of the contract, are not afforded the flexibility of reassignment. So they need to be checked BEFORE access is granted.
If disqualifiers are found, the contracting company must provide you with someone who can have access, or the contract should be considered in breach.

5.12 Policy Area 12: Personnel Security

- ❑ Finger Print based Record Check
  - Finger prints submitted to KBI
    - KBI searches KANSAS records then forwards to FBI
    - FBI searches images associated with III
    - Results will be returned to Agency Primary terminal.
    - QR for any "rap sheet" in III.
    - KFQ for KANSAS CCH.
  - QWA Searches all NCIC persons files without limitations.
  - Out of State?
    - Run Nlets IQ for state of residency.

There are downsides to everything.
Today's name based search capabilities – like "Soundex" - in state and national criminal databases will likely result in "false positives"

Consider a fictitious demographic:

Richard Adam Smith from Fort Wayne Indiana
Date of Birth July 4 1965
Social security number 111-22-9632

A name base search may find lots of Richard, Rick, Dick Smiths (or Smythes, Schmidts, Schmitz, Smits, etc.)
Lots of folks born on July 4th in years before and after 1965.
Or have Social security numbers with many combinations of matching sequences to our subjects.

A finger print based check uses images of our subjects biometrics to search for any matching images in the III (associated to a criminal file).

But, finger prints can't be compared to non-existent images. And some states don't participate by submitting prints to III.
Finger prints are compared to images associated with historical files and not necessarily current wants and warrants in NCIC or state person files.

So do both. Finger print first. Name base next - for non-Kansas resident, use NLets.

5.12 Policy Area 12: Personnel Security

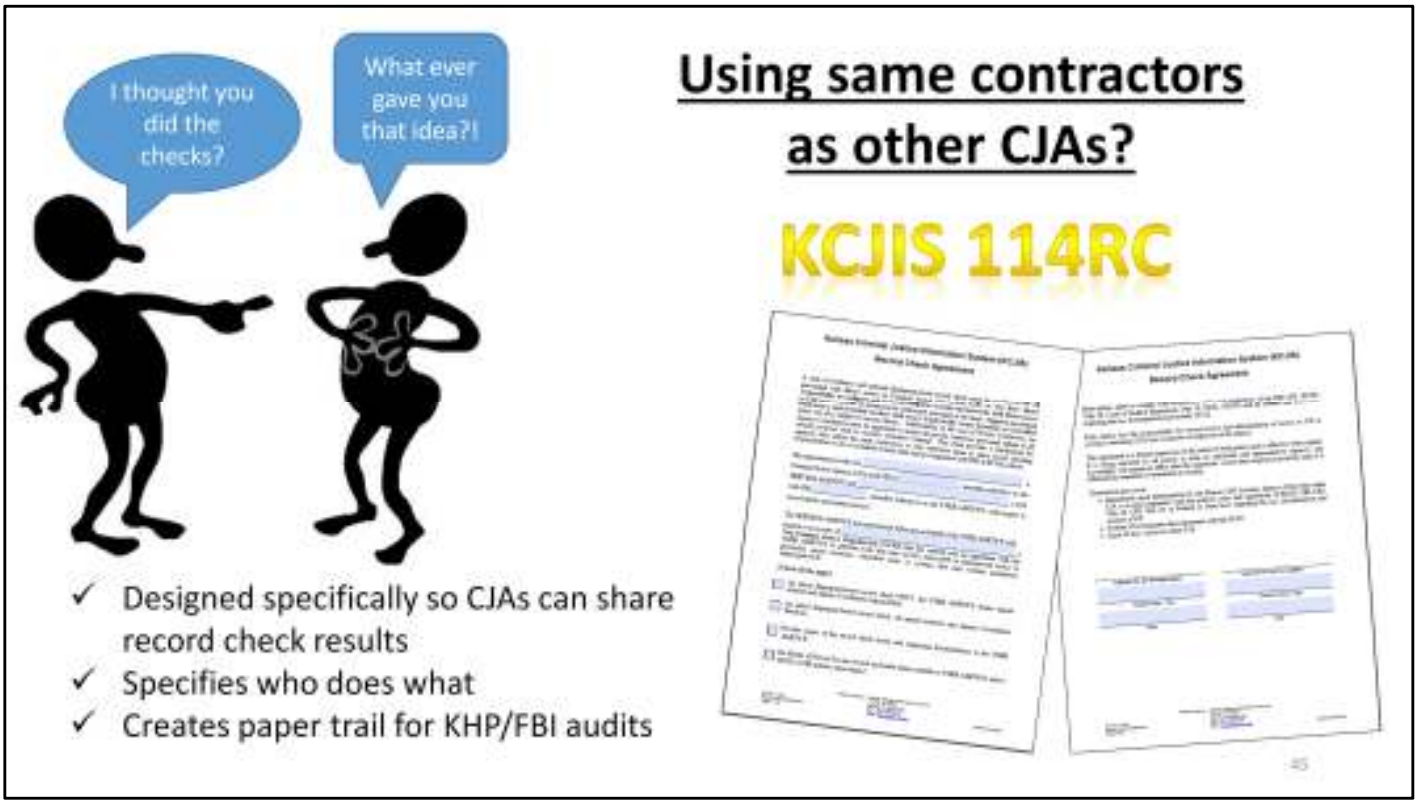
- ❑ Name Based Record Check ANNUALLY thereafter
  (or when reasonable suspicion that CHRI has changed)
  - NCIC Person files (QWA)
  - III (QH)

    (QWI = QWA + QH)
  - Nlets IQ for out of state of residency
  - KANSAS wanted
  - KANSAS CCH

Once your person has been authorized, KCJIS requires annual rechecks in case they got in trouble and didn't tell you.

QWA is ONLY person file query key that will return ALL results available from NCIC for ALL states regardless of extradition.

And, remember to feel free to do more than policy minimums.
Policy only requires checks for criminal record information and that doesn't always give you the whole story.
Personal interviews of their acquaintances and past employers are more likely a better indicator if they can do the job you need.



After conversations with FBI CJIS auditors and ISO staff, the KHP has developed a way to keep the same private contractor employee from having to be fingerprinted multiple times in Kansas.

In a nutshell:

FBI is allowing shared record checks as long as:

1. The CSA (that's KHP) is aware and approves the process

2. A paper trail exists to follow back to confirm they are being completed.

And…

3. They are completed by someone in KANSAS (inTRAstate).

FBI is fine with intrastate sharing. But to this point have not allowed interstate. (Oklahoma can't do your checks for you)

Using same contractors as <u>lots of other CJAs?</u>

- ❑ Contractor has ***3*** *or more* CJA customers.
- ❑ Contractor has ***6*** *or more* employees.
- ❑ CJA customers spans jurisdictions.

47

KANSAS HIGHWAY PATROL
CJIS Unit

Kansas Criminal Justice Information System (KCJIS)

Record Check Agreement

A state of residency and national fingerprint-based record check must be conducted for all personnel with direct access to Criminal Justice Information (CJI) or who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI unless escorted or monitored by authorized personnel at all times. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas are also subject to record checks. Additionally, in the case of Private Contractors, an Agency Coordinator must be appointed to ensure all private contractor personnel adhere to all security policies such as security awareness training. This form provides a mechanism for agencies who utilize the same contractors or who otherwise agree to share record checking responsibilities to do so on behalf of each other and in compliance with FBI & KCJIS policies.

This agreement is between the Kansas Highway Patrol (KHP), a Criminal Justice Agency (CJA) with ORI of KSKHPQ000, and _____,
a CJA with ORI _____ (henceforth known as the AGENCY).

In regards to associates of _____,
a Non-Criminal Justice Organization (NCJO) that has entered into an agreement with the AGENCY to perform work that may involve unescorted or unmonitored access to physically secure locations, controlled areas or systems that may contain unencrypted, unredacted CJI.

On behalf of the AGENCY, the KHP shall perform the following:

- ✓ An initial fingerprint-based record check, all annual rechecks and Agency Coordinator Functions.
- ✓ Be Holder of Record for any records and make them available to AGENCY FBI auditors upon request.
- ✓ The KHP shall review all records obtained as part of this process and adjudicate (approve or deny) the subjects access to CJI or systems containing CJI. All adjudications shall be communicated to both the Agency and NCJO through electronic means as marked below:
  - ☐ Email
  - ☐ CJIS Online
  - ☐ Other method: _____

As side effect of state level initiatives, the KHP has managed to obtain some funding to help everyone out.

PLEASE…
the FD 258 needs to be:

- **LEDGIBLE**
  - Livescan/ machine printed preferred
  - FULL images
- **COMPLETE**
  - LAST, First, Middle
  - Date of Birth
  - Place of birth
  - SOC
  - CURRENT Residence (State)
- **CURRENT**
  Image capture date MUST be within past 12 months

  KHP has cards with our ORI

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

6. Be responsible for securing security awareness training and associated record keeping.

5.2 Policy Area 2: Security Awareness

- "roamin' around" access to areas where CJI is processed or stored. 5.2.1.1 (1-4)
- ACCESS to plaintext(unencrypted) CJI. 5.2.1.2 (1-6)
- Physical and logical access to CJI (computer access) 5.2.1.3 (1-17)
- Unmonitored access to networks used to transmit unencrypted CJI. 5.2.1.4 (1-5)






CUMULATIVE

Think of anyone with access to areas or systems where CJI is processed stored, or transmitted as extra eyes to look out for problems.
Like a "neighborhood watch" within your building or network.

It starts with EVERYONE knowing some foundational security practices even if they are just "passin' through" :

1. Individual responsibilities and expected behavior with regard to being in the vicinity of CJI usage and/or terminals.
2. Implications of noncompliance.
3. Incident response (Identify points of contact and individual actions).
4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.

As a person's access to CJI increases, so do the awareness topics.

If the process of completing security awareness seems too daunting, it can be reduced by reducing the number of people with access to unencrypted CJI and places it may be found.

5.2 Policy Area 2: Security Awareness

- BECAUSE.. People are the weakest link!

❑ KHP CJIS Launch Pad

+

❑ NexTEST tracks CJIS requirement

If you are still doing things on paper, consider NexTEST.
It tracks a user's completion of a test and when they are due to repeat the training.
As the vendor brings on new features, we will consider incorporating them to make all our lives easier.

For now, be sure users are getting the CJIS Security & Awareness box checked under "Other Certifications" at the bottom.

If your agency is a D.I.Y. place, your auditor will review your curriculum and tracking process for compliance to policy 5.2

Vendors from out of your area?

Has lots of employees?

Used by several agencies?

INTRODUCING!

- ✓ FREE to local agencies.
- ✓ From the makers of NexTEST.
- ✓ Designed for non-agency personnel. (No KCJIS user required).

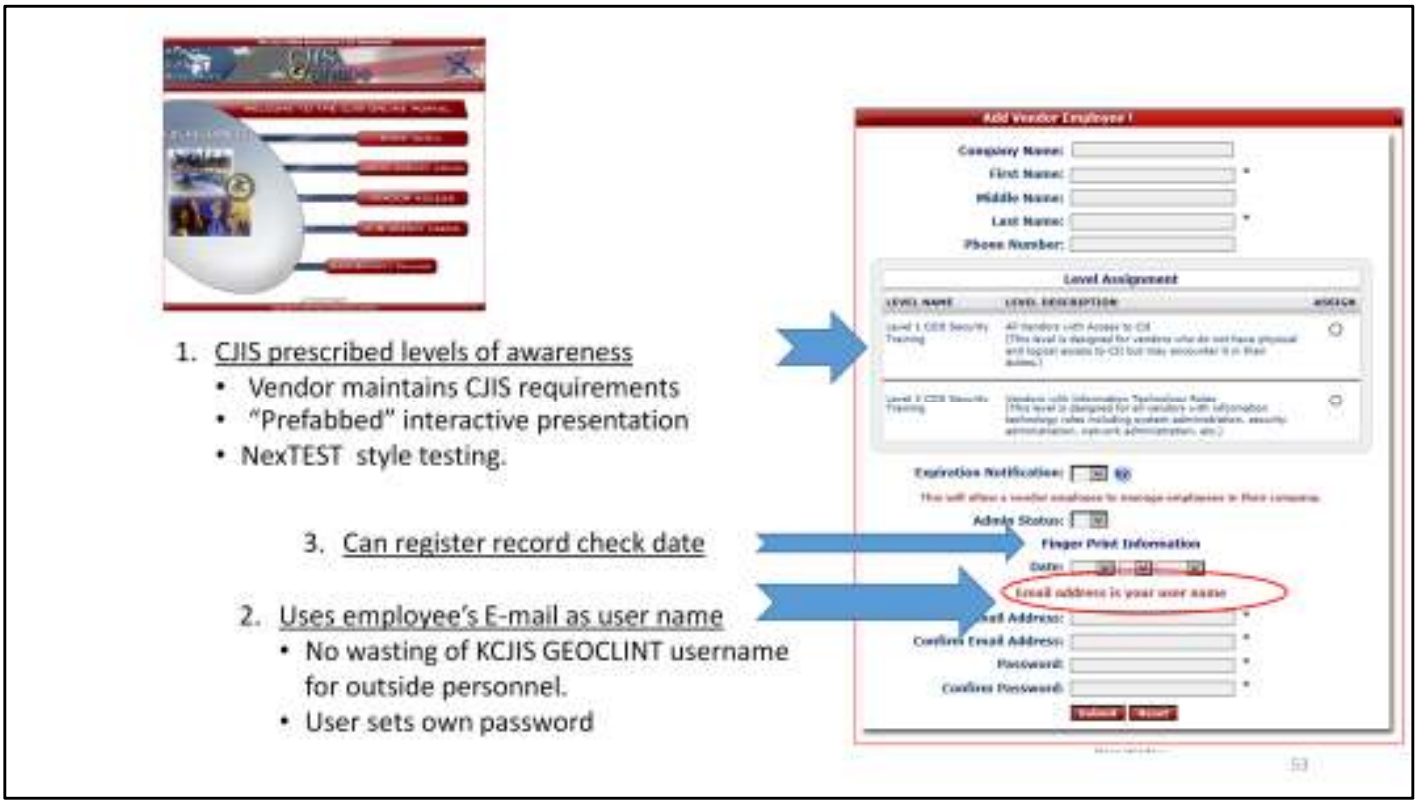
Contact your I.T.S. auditor for details

If you have several NON-AGENCY personnel
- accessing unencrypted CJI or
- with access to your network used to transmit unencrypted CJI,

KHP has purchased the CJIS Online product.
This is a FREE TO AGENCY way to track contract employees' security awareness training.

Used in several states and has been seen by FBI auditors.

AND the information is online so ALL agencies can share.



1. As FBI levels and topics change, the CJIS Online vendor will update software materials accordingly.

2. Uses Email address for user identification so NO KCJIS USER ID REQUIRED.
   - NOT agency specific so contractor employee completes ONE TIME to satisfy biennial requirement for ALL agencies across the ~~state~~ **country**!

3. Fingerprint record check date can be entered so ALL state agencies know.
   - Coordinate through KHP CJIS I.T.S.A. team

5.5.4 System Use Notification

At the operating system level, OR....

WARNING! – FOR OFFICIAL USE ONLY.

You are accessing a restricted information system.

System usage may be monitored, recorded, and subject to audit.

Unauthorized or inappropriate use of the system is prohibited and may result in discipline up to an including dismissal from employment, civil and/or criminal penalties that may include prosecution.

Use of the system indicates consent to monitoring and recording.

At the application level

We need to make sure users are being warned of consequences of their misbehavior.

Similar to password policy, the system use notification can be implemented at various levels PRIOR to accessing CJI systems.

Consider having such notices at All levels as they proceed into their device, and then into your CAD/RMS and other systems containing critical or sensitive information.

Questions regarding shredding company continue to be asked. Remember the SCOPE of policy concerns when evaluating use cases such as this one.

- The WHAT needs protected - unencrypted CJI - exists.
- The WHERE is NOT a physically secure location (NOT under management control of a CJA).
- The WHO is a contractor, so policies about access to ANY unencrypted CJI applies for ALL of the company employees or subcontractors who may access unencrypted CJI.

    - ❑ FBI CJIS Security Addendum referenced in contract (5.1.1.5, APPENDIX H)
        - ❑ Certification page signed by each company employee
    - ❑ Record checks (5.12.1.2)
    - ❑ Security awareness training (5.2.1.1).

What other polices would an offsite shredding vendor need to be reviewed against?
5.3 incident response to a small extent - (the what if train hits the truck on way to shredder scenario)
5.5.2 Access enforcement (see 5.8.4 below)
5.8.2.2 Media Transport
5.8.4 disposal of physical media (those who can unlock the bins need to be "authorized" that is record checked and security aware trained).
5.9.1.2 ; 5.9.1.3 ; 5.9.1.8

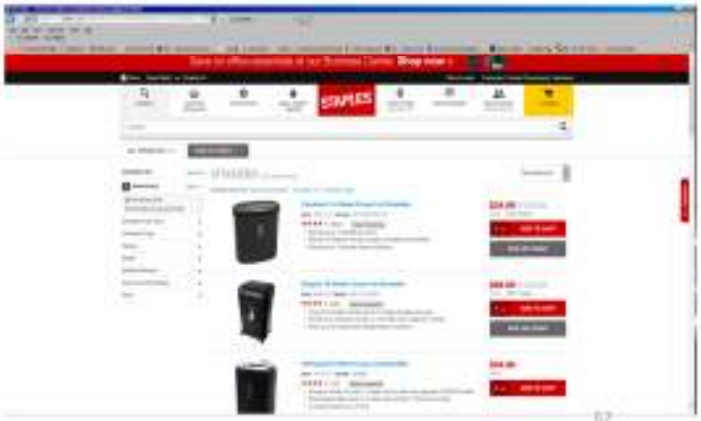
5.8 Policy Area 8: Media Protection

5.8.4 Disposal of Physical Media

Authorized User/Personnel — … who have been appropriately vetted through a national fingerprint-based record check …

POLICY MITIGATION OPTIONS:

- Change contract for on site shredding where an agency authorized person witnesses the shredding.
  - Search Onsite Shredding



Cost too Much?

- Go paperless.
  - Search Print to PDF
  - Copy + Paste to other application
- Buy a shredder
  - shred your own documents containing CJI.
  - Destroy A.S.A.P. (see 4.2.4)

Paper work too much of a hassle?

On site shredding will be more expensive. ☹

Utilities are available for Windows and other operating systems that are treated like a printer by the O.S. that can convert your data to Portable Document Format (PDF) for digital storage. Encryption standards apply (see 5.10.1.2) but may be cheaper and easier to deal with at end of use destruction time than paper shredding.

Cross – cut shredders will provide enough destruction to satisfy policy requirements. And they don't have to cost much.

Per Policy 4.2.4 actual CJI "… shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files."
In short layman terms: keep it only as long as you need to for the case adjudication process. Then get rid of it.

If you're like many of us, that will require a change of habits!

After years of debate or discussion, the FBI CJIS Advisory Policy Board decided that a vehicle that can be locked is physically secure enough to be treated like a brick and mortar location.

Physically secure locations control access to personnel:

- Authorized (those who have been properly vetted) and approved to be there alone.

Or

- Escorted by authorized personnel.

The authorized person can control what the escorted person can see, touch, and hear by stopping and/or redirecting a visitor's path, close an MDT screen down or invoke screen saver, etc.

The concepts of physical security can be analogous to your computer operating system's services and processes.
Physical security is dependent on:

- Security Awareness (5.2)
- Access Controls (5.5)
- Identification and Authentication (5.6)
- Personnel Security (5.12)

Without proper implementation of these other policies, there is no physically secure location.

Conversely, proper implementation of physically secure locations affects whether

- Advanced Authentication (5.6.2.2)

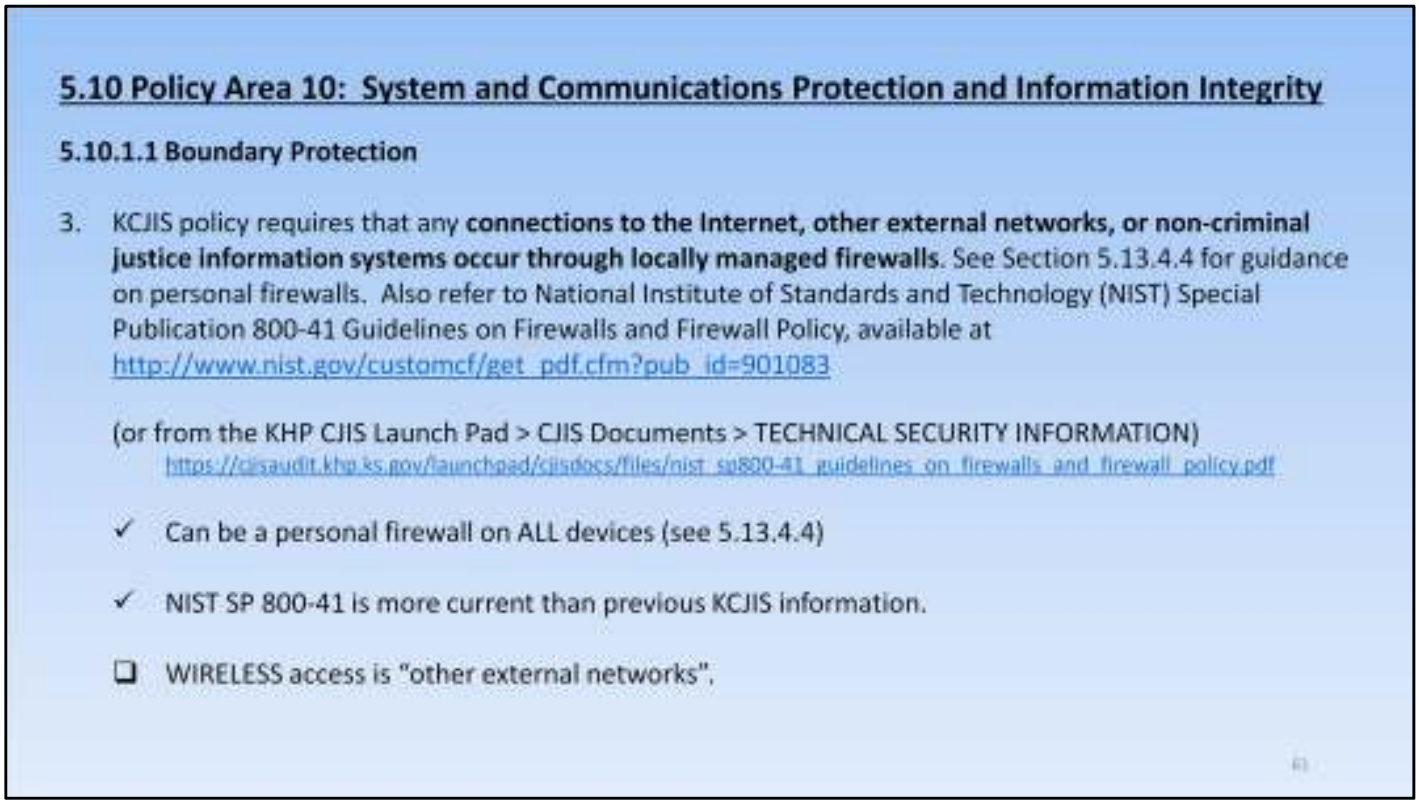
Or

- Encryption (5.10.1.2)

Are required.

Unlocked facilities – regardless of their building structure are NOT physically secure.

Neither are brick and mortar that allow unescorted visitors.



KCJIS' 5.10.1.1(3) is stronger. NOT new to KCJIS **– we've always required firewalls**. Industry best practices and the characteristics of the CJIS security policies requirements make a firewall the best choice for protecting your boundary.

"Other external networks" covers Wireless Access.

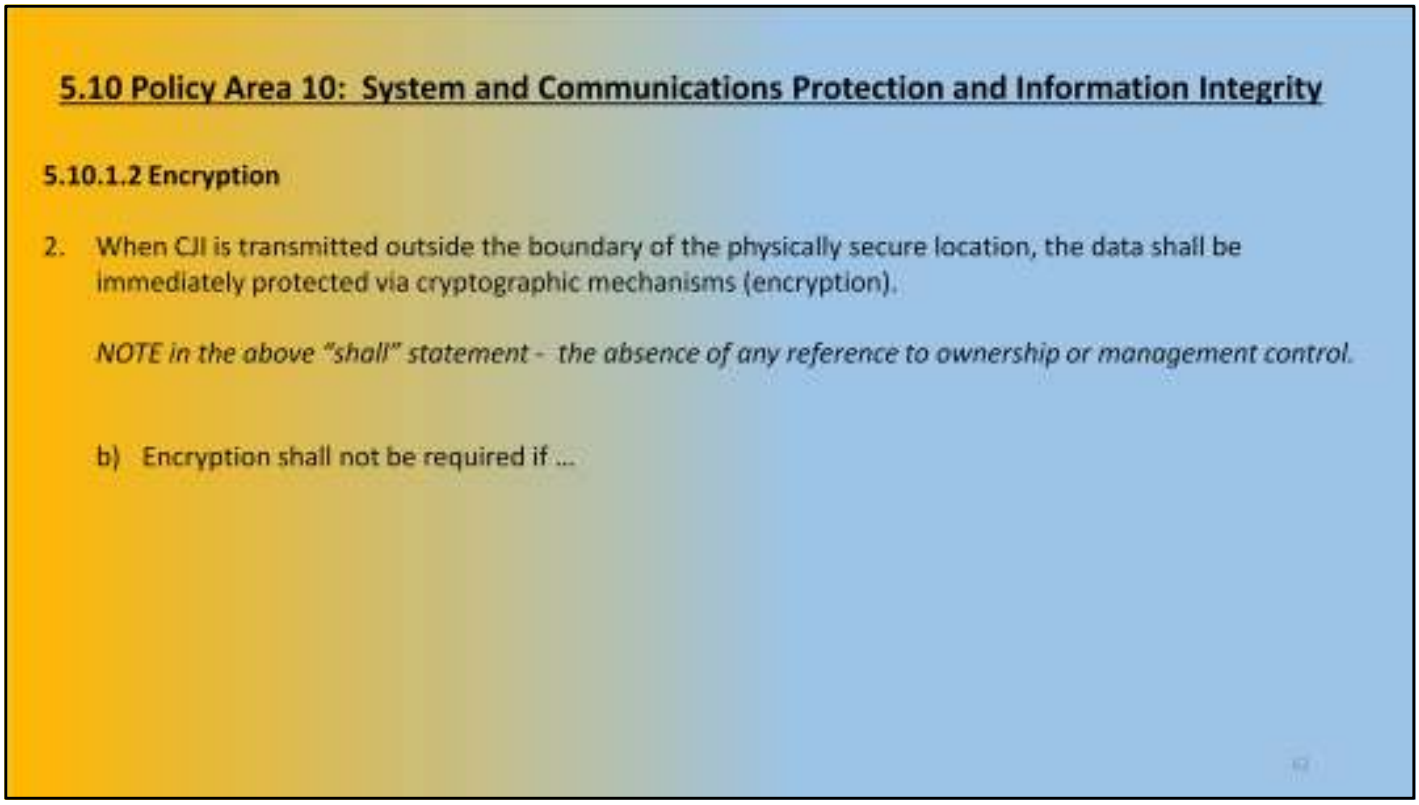
What IS new for KCJIS is the elimination of a "shopping list" of firewall requirements. Instead, we now refer to a NIST special publication.

A personal firewall on ***ALL*** devices is allowed in place of a network appliance firewall.

As LASO you need to have a good working relationship with your I.T. staff that manage the firewall(s).

Policy is specific that if the device has issues (fails) that nothing gets through.
In other words, "if all else fails, block the access".

If you were to install a brand new firewall, for example, it should start out in a default mode to block everything. Then I.T. will need to configure specific rules to allow operational needs to pass through, while everything else remains blocked.



Policy requires digital CJI to be encrypted ***when it is being transmitted*** beyond your physically secure location, ***REGARDLESS of who owns or controls the cable runs*****.**

Older FBI policy exempted encryption if the cable was "under management control" of the CJA. But that changed in FBI policy 5.0.
We failed to recognize the subtle change until the 2014 FBI audit. So we need to call everyone's attention to it.

There are some exceptions…

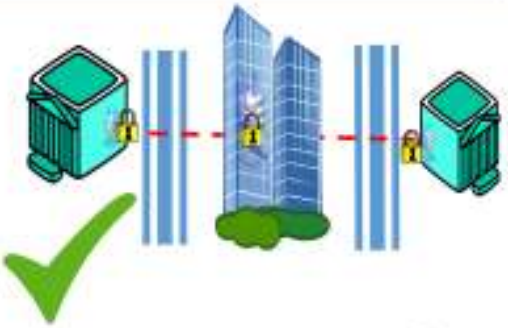
Secured CAMPUS

1. Agency controls all areas where cable may be buried.
2. All cables terminate within physically secure locations.
3. All possible paths of buried cable between are in line of sight.
4. **EXEMPT from encryption requirement**

Government Center

Two CJA facilities about 1 block apart. Separated by NCJA (government) building. Government owns and manages fiber.

1. CJA does NOT control all areas where cable may be buried.
2. All paths of cable between are NOT in line of sight.
3. Cables run through concrete and other impenetrable "conduit" into secured facilities (wiring closet or server room) under control of I.T.
4. CJA has MCA with I.T. so all personnel with access are under CJA control.
5. **ENCRYPTION IS NOT REQUIRED**.



Encryption is NOT required IF Your agency owns or manages all of the transmission facilities and can guarantee the physical security of those facilities

i.e.: Agency always has management control over the physical and personnel who can access the transmission facilities.
Or the lines are incased in some protective housing that physically prohibits access - such as concrete.

In the correctional facility scenario:
All CJA controlled ground between buildings. Everything is in line of site.
Nobody is going to dig up your line without your knowledge.
NO ENCRYPTION REQUIRED.

In this Government Center MAN scenario,
Cables running in protective environment making attempts for unauthorized access impractical to impossible
EXEMPT from encryption requirements.

This may be easier said than done (and words are cheap). Search internet for "Protective Distribution Systems".
Encryption may actually be the simpler, more flexible, and less expensive option.

Government Center
Two CJA facilities about 1 block apart. Separated by NCJA building.
Government owns and manages fiber.

1. CJA does NOT control all areas where cable may be buried.
2. Some cable runs through public access plenum in middle building.
3. Some cables terminate in NCJA areas of middle building.
4. All paths of cable between are NOT in line of sight.
5. There is no controlled campus.

ENCRYPTION IS REQUIRED.

Metropolitan LAN
Two county facilities separated by about 1 mile of uncontrolled city area. County owns fiber.

1. Agency does NOT control all areas where cable may be buried.
2. All paths of buried cable between are in line of sight.
3. BUT… Even if there may be line of sight, there is no controlled campus.

ENCRYPTION IS REQUIRED.

In this Government Center MAN scenario,
The CJA cannot control all areas of potential access to cables.
ENCRYPTION IS REQUIRED.

Metropolitan Area Network (MAN):
Cable runs through non-CJA controlled space.
Because CJA cannot control who digs, even though line of site is there,
ENCRYPTION IS REQUIRED.

5.10 Policy Area 10: System and Communications Protection and Information Integrity

5.10.1.2 Encryption

3. When CJI is <u>at rest</u> outside the boundary of the physically secure location,

   a) … the **passphrase used …** shall …: (be at least 10 characters from all character groups)

Pampers

(Changed when user no longer needs access)

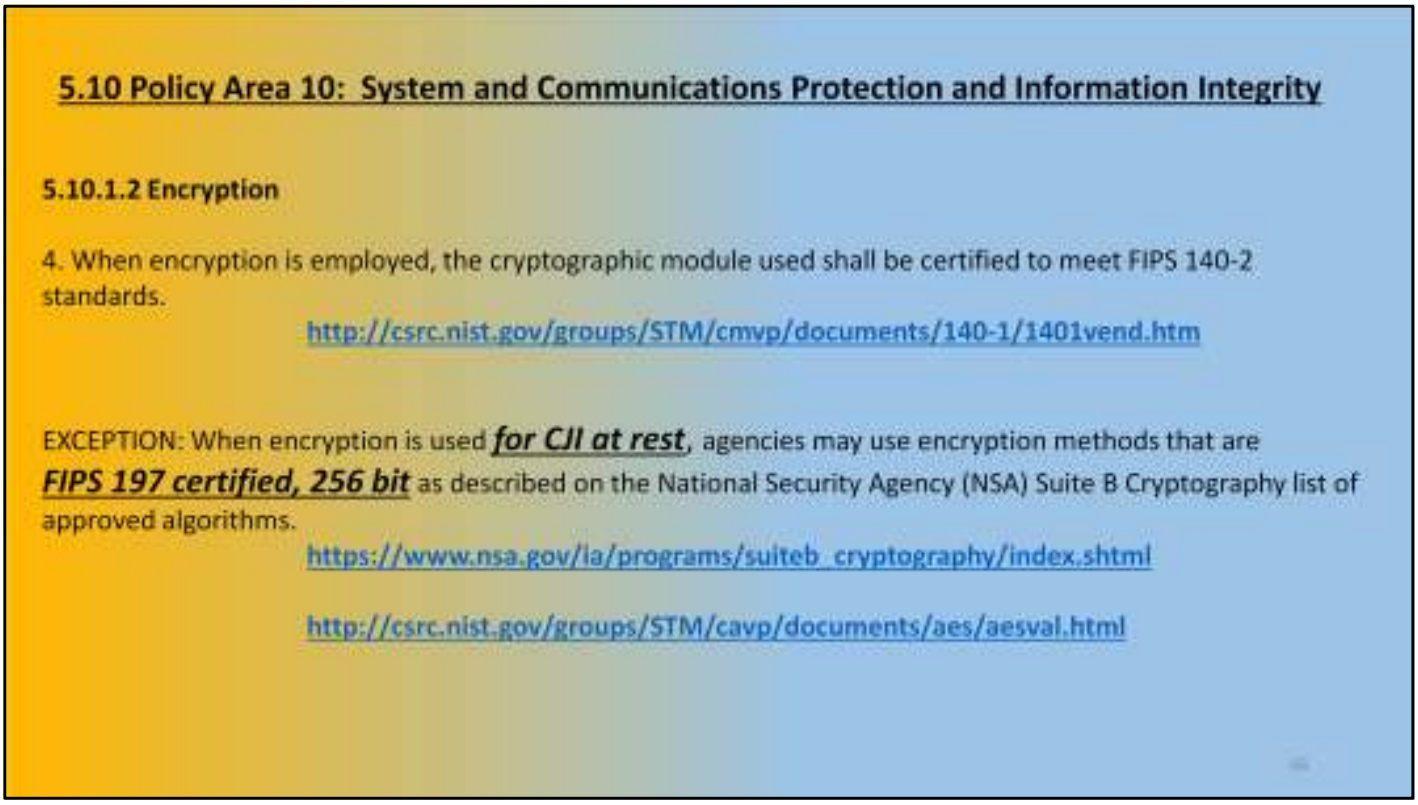
   b) Multiple files in the same unencrypted folder shall have separate and distinct passphrases. *<u>A single passphrase may be used to encrypt an entire folder or disk</u>* containing multiple files. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied.

CJI at rest can be treated a little differently than in transit.
A FIPS 140-2 certification is an option, **but not needed IF**
the encryption is **NIST certified AES-256** with robust passphrases.

Passphrases are NOT same as passwords.

- Passphrase in 5.10.1.2 (3.a.) does NOT authenticate an individual
  – anyone who knows the passphrase can access the data.

- Passphrase construction in 5.10.1.2 (3.a.) is stronger than 5.6.2.1.1 password requirements.



To review:

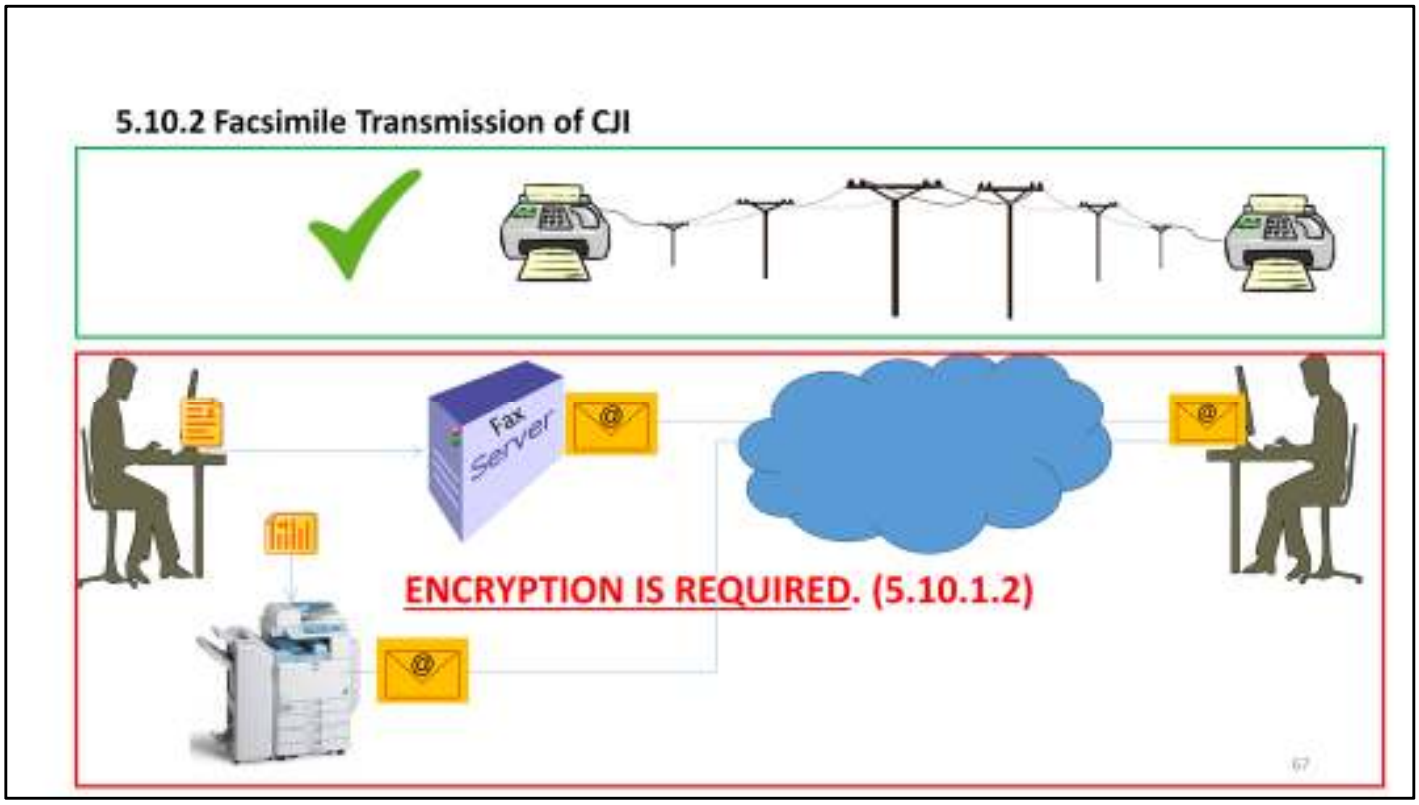
Policy requires digital CJI to be encrypted to FIPS 140-2 when transmitted beyond your physically secure location , **REGARDLESS of who owns or controls the cable runs.**

The National Institute of Standards and Technology (NIST) publishes a website that lists encryption ***modules*** that have been tested and are certified to meet FIPS 140-2 . *Modules* are how the encryption vendor has combined approved algorithms with key management and other security features to ensure the encryption meets FIPS 140-2.

A variance (sort of) is allowed for data at rest.

The NSA Suite B currently defers to NIST/FIPS 197 (AES-256) for the actual algorithm used to encrypt the data. The NSA link on the slide has a table showing other specifics for key management, digital signatures, etc.

The second NIST link is the list of products that have been tested and certified to properly implement the AES algorithm described in FIPS 197.

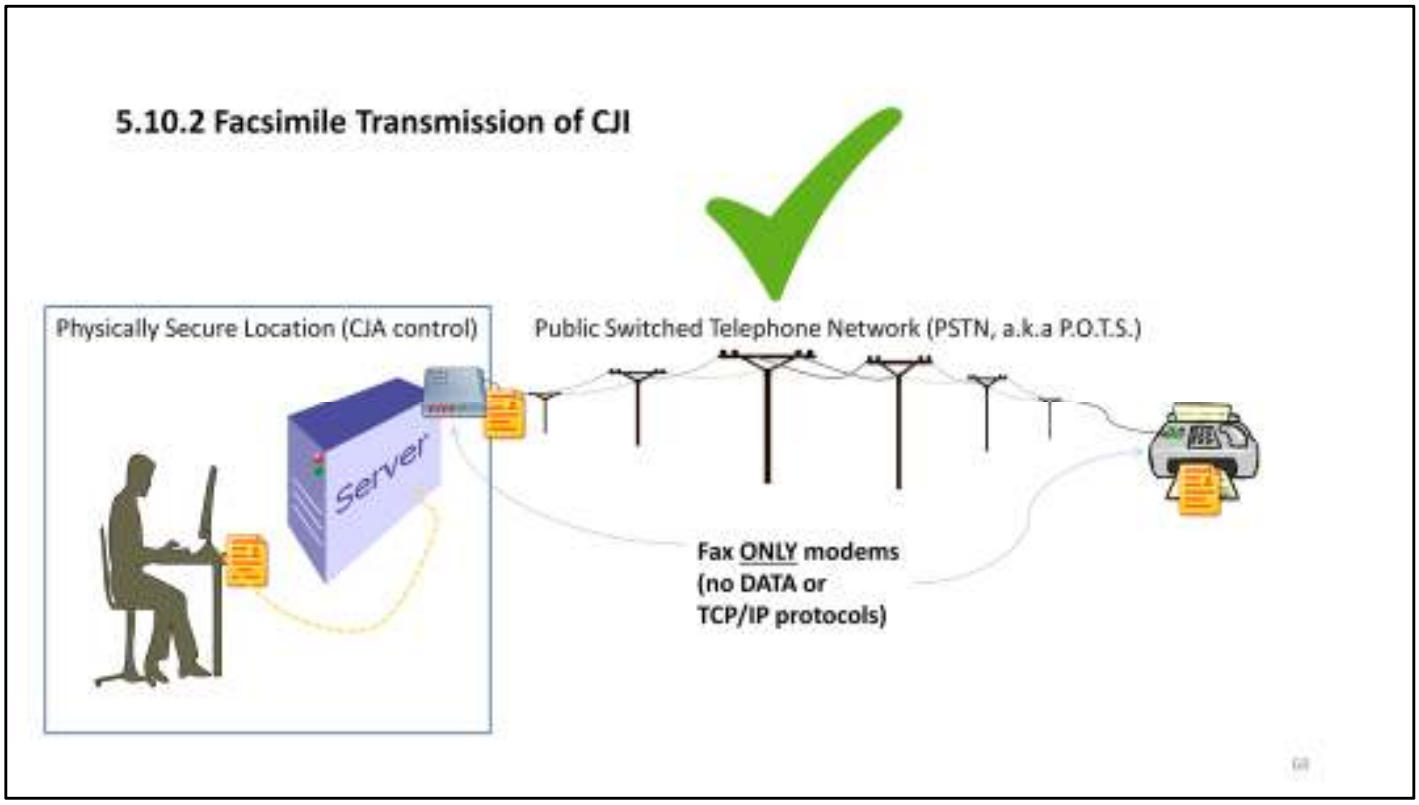


<u>Old school stand alone fax machine to stand alone fax machine is exempted from the encryption requirement.</u>

However, if your "fax" is a TCP/IP network based or cloud based solution, to look more like email, using TCP/IP protocols, such as:

- Facsimile software (local install or client/server)
- Multi-function printers with scan to email feature

then encryption ***<u>IS</u>*** required.



If your agency has a fax server in house and:

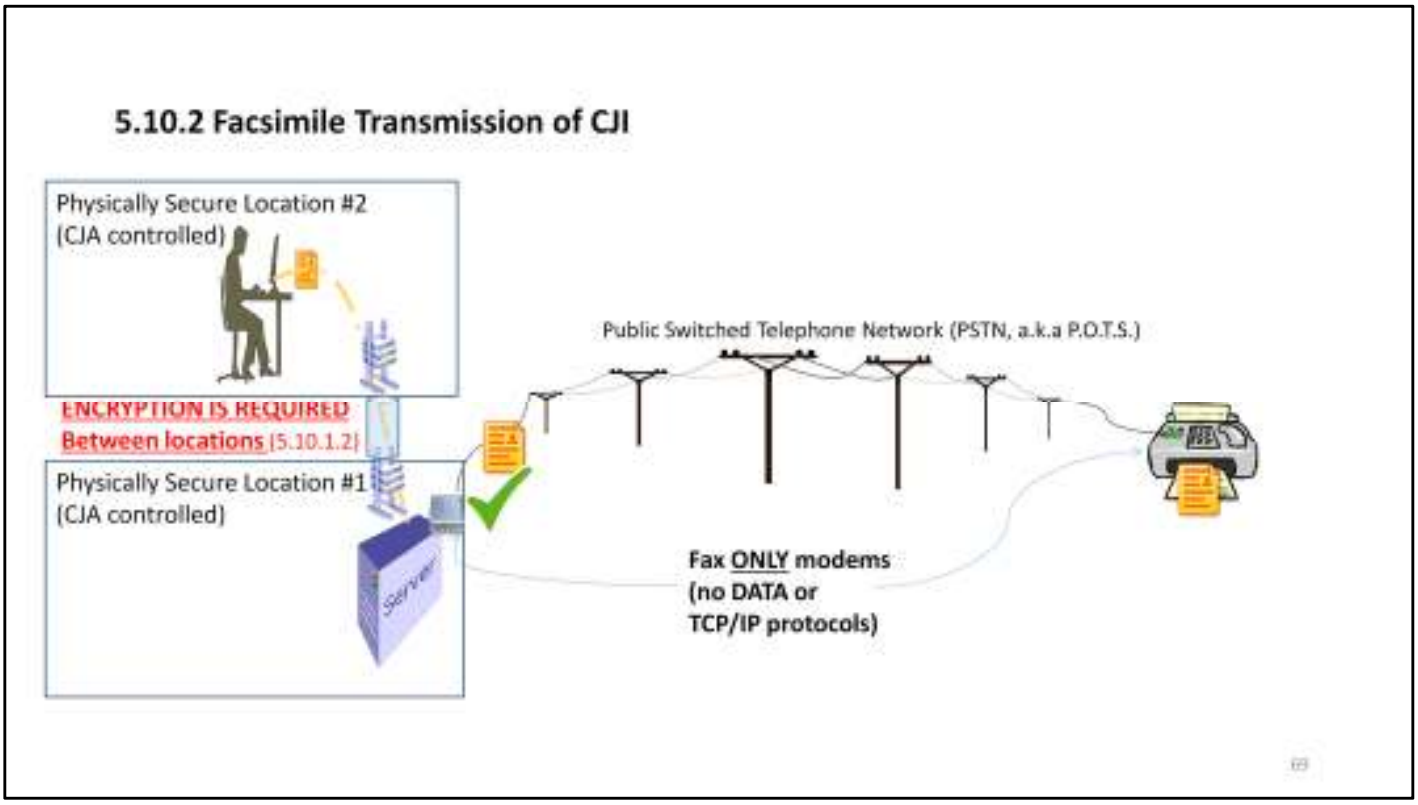
- There is only 1 location.
- The server and network are operated in a physically secure manner.
- The server uses a FAX ONLY modem*.

*FAX modems differ from DATA modems because all they can do is send a converted image of a printed page over phone lines.

Your users execute a program or software add-on from their computer to connect over your secured network to the fax server.

The server acts like an old school fax machine to send the image over phone lines (NOT via internet).

This arrangement is OK and EXEMPT from the encryption requirements.



But what if you have remote locations connected over a MAN?

Fax server is located and operates within one brick and mortar physically secure location like previous scenario.

But users in the other remote location(s) connect to the fax server via TCP/IP protocols.

The connection between your locations requires encryption as we have already discussed.
Email,
Files transmitted to network storage,
And “Fax” via the server.

5.10.1.5 Cloud Computing

Review the cloud computing white paper (Appendix G.3), the cloud assessment located within the security policy resource center https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view, NIST Special Publications (800-144, 800-145, and 800-146),as well as the cloud provider's policies and capabilities will enable organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy.

Does your agency think it wants to "be in the cloud"?.

It can be OK , as long as you jump through all the hoops.

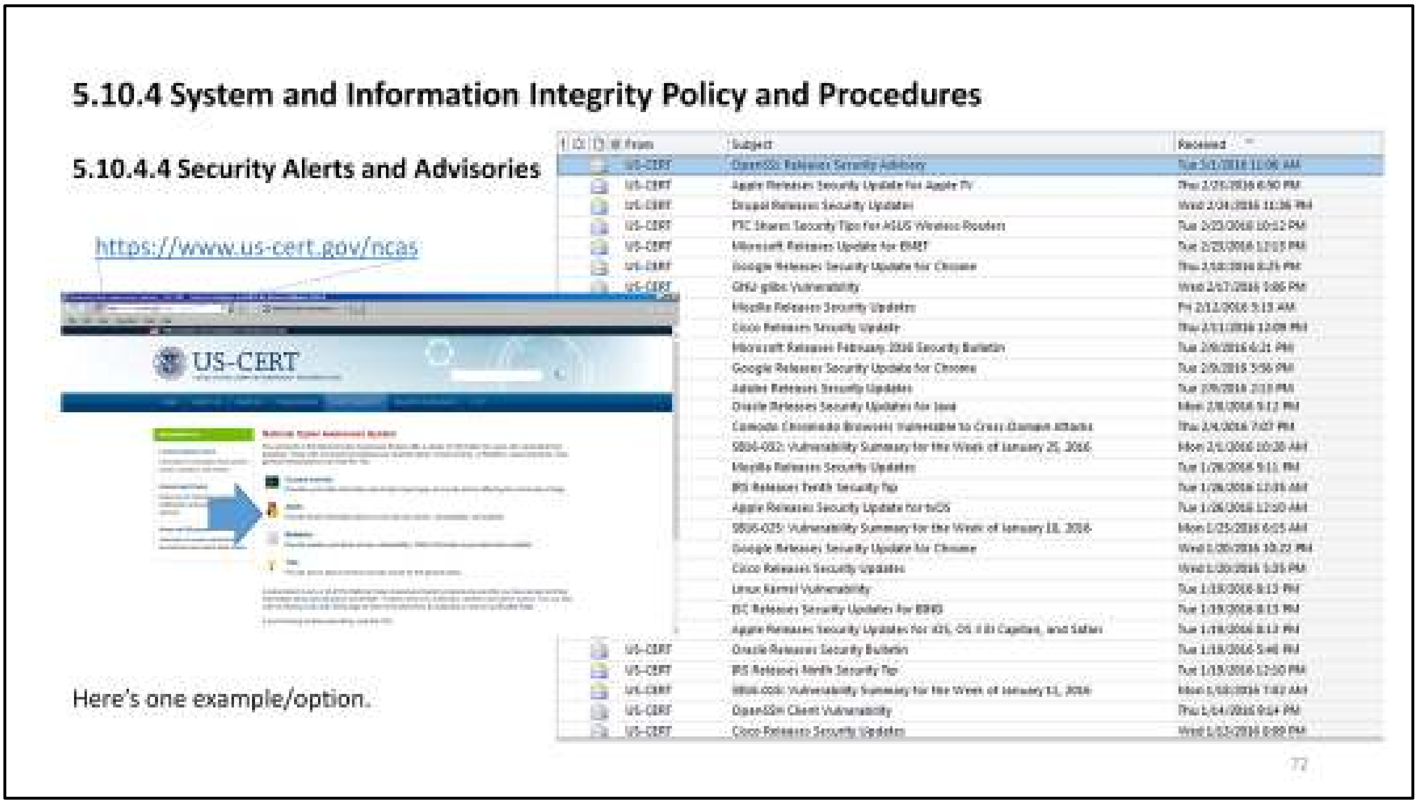
The FBI offers some resources.

- Policy Appendix G.3
- Their policy resource center website has 2 documents.
  - The cloud computing report is the discussion document about all the factors to consider.
  - The CJIS Control Catalog contains the security control requirements from the CJIS Security Policy and addendums to each control applicable to either the agency obtaining cloud computer services or the cloud computing provider

Suffice it to say, it can be done, when ALL Security policies are accounted for and enforced. KHP CJIS may be able to help with the "administrative" tasks of the "Agency Coordinator")see record check and security awareness sections of this course).

BUT – ***the local agency is responsible*** to ensure ***THEIR*** setup/configuration/implementation of the cloud provider services are done in manner compliant to policies.

Ask before you jump – or you might get burned!

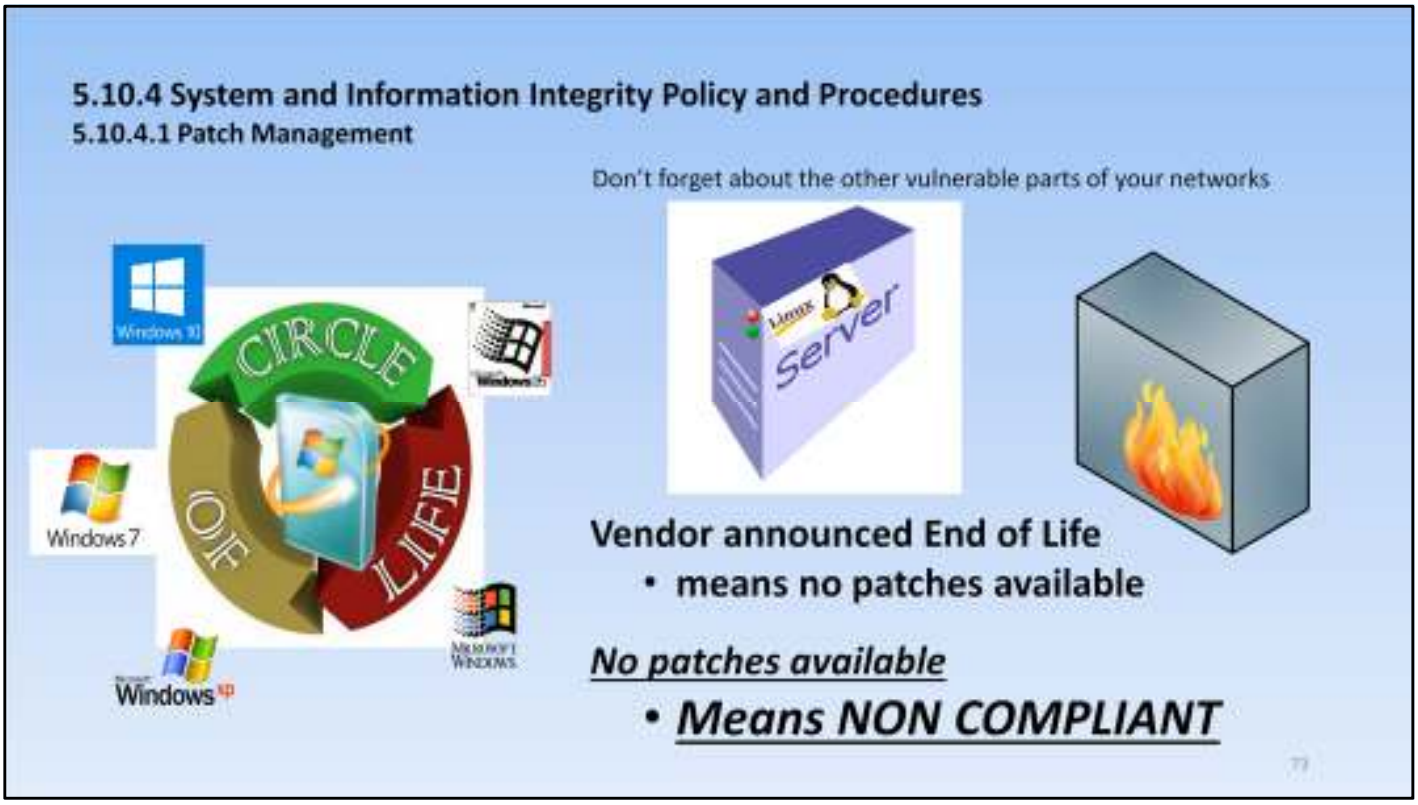


Part of patch management is knowing about the vulnerabilities needing patched.
Because the bad guys likely know 'em already, you need to find a way to be alerted.
Viral outbreaks of malware or other breaches are sometimes likely determined by how lucrative the breach can be versus how hard it is to carryout.

This screen shot of an email alert inbox is just a small sampling of the alerts available in a few short weeks.

US Cert is a good resource for these alerts. But others are out there as well.
Your security vendors may also offer alert services.

Once you have alerts coming, your are likely to notice that NO VENDOR is exempt.
So don't let anyone tell you they don't have malware problems.
They are either extremely lucky, or their market share is so small that the crooks don't waste their time.

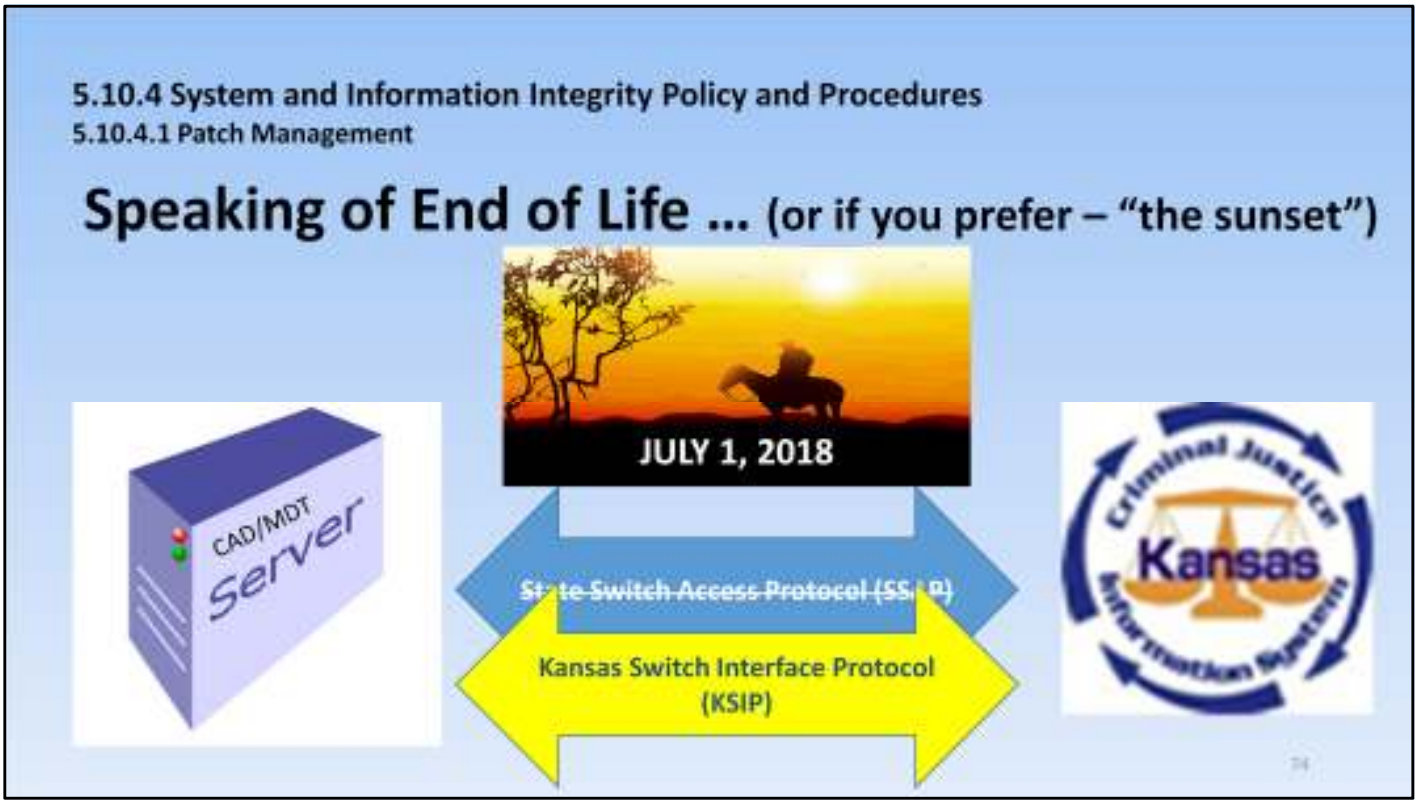


Products have lives. Equipment and software makers move on and leave their old stuff behind. As LASO – be familiar with the products used on your network connecting to KCJIS (policy 5.7). Be aware of when those products are outdated …
… or have issues that need fixed.
Know your vendors' vulnerability notification and patch policies. (Which do they announce first – the vulnerability or the patch? Or does it depend on seriousness?) Either way, be on your toes and get the holes patched A.S.A.P.

Patch management can work on the concept of "defense in layers". For many vulnerabilities more than one condition must be present. For instance, a targeted application must be at a certain level or version and be installed on a device running a certain version of operating system. Patching either the program or the operating system, will block that particular vulnerability. BUT THERE MAY BE MORE!

Have you ever had to call a plumber to fix a leak? In the course of repairing the obvious break, did they wind up breaking the other water line?

In plumbing and in patch management, the process needs to be able to test for additional issues and be prepared to repair those things the fix either caused or brought to the surface.



Effective July 1, 2018, the KBI Help Desk will no longer support the legacy SSAP protocol.

ONLY THOSE SERVERS AND TERMINALS USING THE LEGACY SSAP protocol will be disconnected from the Central Message Switch on this date. *OpenFox Terminals or systems using the KSIP Protocol will NOT be affected*. The KBI has been contacting affected agencies, but if you are not sure if your agency is using the legacy SSAP protocol, please contact the KBI Help Desk and ask.

If you wish to continue your server connection through the Central Message Switch, you will need to update your SSAP protocol servers and terminals to the new KSIP Protocol before July 1, 2018.

Part of the conversion to KSIP will require certification through the KBI Help Desk.
Please review the Interface Developer Packet 1.1 on the KCJIS Web Portal, specifically section IV. Procedure and Action Steps. ***The process to convert to the new KSIP Protocol can take up to 2 months*** depending on the knowledge of your vendor. You are encouraged to schedule testing times with the KBI Help Desk in advance to ensure timely testing and review of your submitted data. If you have any questions, feel free to contact the KBI Help Desk. You will need to coordinate with your vendor and provide them the necessary documents to convert your SSAP server to KSIP. Here is a complete list of documents to provide to your vendor:
Interface Developer 1.1
Kansas Message Key Book 6.1
KBI Vehicle IEPD_1.2
KBI_DL_IEPD_1.0.9
KCJIS Central Message Switch Developer Guide 1.1
NLETS NIEM 4.1 Schema
OFML Interface Specification 2.0
OpenFox Foxtalk Specification 1.1

5.10.4 System and Information Integrity Policy and Procedures
5.10.4.1 Patch Management

Unless you have a

You Need A Budget.

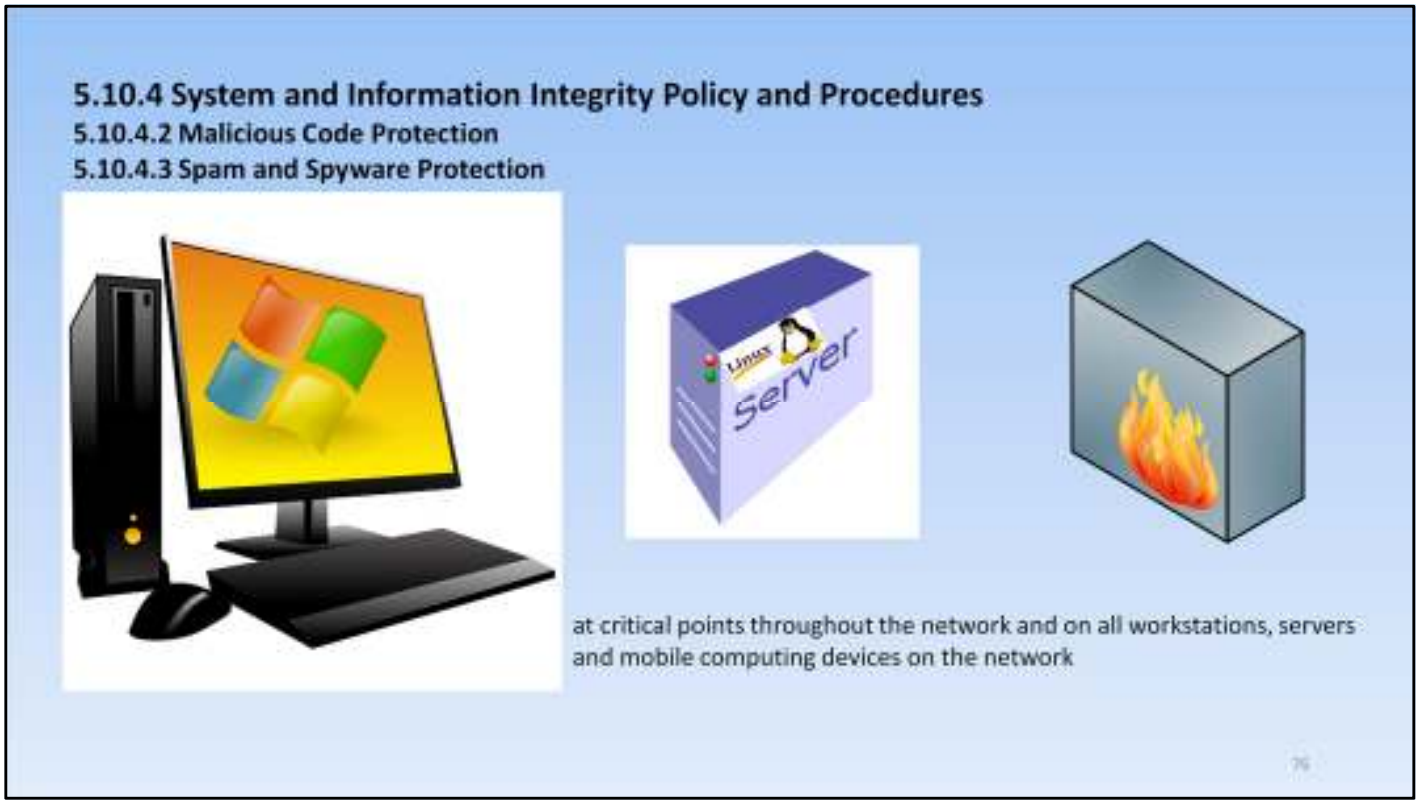
for Equipment and software upgrades and support ***after*** initial funding and contract expires

EDITORIAL COMMENT HERE…

BEWARE! There is no such thing as free money.

GRANTS are to budgets … as OPIODS are to pain.

They provide a temporary solution or relief of a pain.
BUT THEY RUN OUT or EXPIRE.
Then the pain come back – sometimes stronger than before.



Neither the FBI or KCJIS mandate any specific "brand" of security software be used.
Your product should reflect your agency needs with insight from your I.T. professionals.
Depending on which review you read as to which is best today. Will be different next review.
How each application performs updates and protects in "real time" will vary by their design.

- Most anti-virus products offer multiple updates each and every day. Yours should, too!
- Some utilize "cloud based" databases lists. That is OK, but be sure there is something available locally on the device when the cloud isn't.

Some security "suites" combine Anti-virus, host-based firewall and Intrusion Detection, and mail filtering into a single product install.

Mobile devices are treated differently due to their limited function Operating systems.

- Check out policy 5.13.2 & 5.13.3

Heuristic and other "real time" features can scan as files are accessed – regardless of where they are located. They don't depend on huge list of virus signatures to compare against. Rather, they look for irregular behavior or activity that is common to malware.

5.13 Policy Area 13: Mobile Devices

Accepted FBI CSP as written *with one addition to 5.13.1.3 Bluetooth*

*Bluetooth is not allowed for transfer of CHRI * between computing devices. Bluetooth is allowable for devices such as keyboards, mice, microphones, headsets, etc.*

*Refer to definition of CJI in 4.1

- Data entry is NOT CJI (yet)
- Devices that display graphic representation of query result (such as traffic light ) are OK
- E-Ticket printer
  - Subject's name, License #, etc. is same information on hand written ticket.
  - CJIS systems are not usually required to obtain that information.
  - Information on ticket does not reveal additional PII, CHRI, or FBI restricted file information.
  - Printer's format not conducive to additional information like CHRI.

77

With approval of KCJIS Policies and Procedures version 5.4

KCJIS has chosen to ride the FBI's coattail on mobility policy with just one addition regarding the FBI's lack of direction about Bluetooth.
Bluetooth does NOT encrypt to the levels of FIPS 140-2. And, as FBI policy states, it is susceptible to many of the same risks of any other wireless connection.

But, it does have a limited range - generally about 30 feet. And it does use a pairing process to mitigate uninvited participation.

Remember the scope of what the policy covers.

5.13 Policy Area 13: Mobile Devices (+ Appendix G.4)
Includes all wireless considerations.
5.13.1.1 All 802.11 Wireless Protocols
5.13.1.2 Cellular
5.13.1.3 Bluetooth
By its nature, wireless communications occur over "external networks" (AIR is *outside* agency control!). See 5.10.1.1 #3 regarding firewalls.

Almost every kind of electronic gadget these days has some kind of wireless connectivity capable of internet access.

Televisions, printers, security cameras, thermostats, electronic door locks, smoke detectors … the list of the "internet of things" can be exhausting and may prove tricky or compromising.
Be aware of these things in your office and be sure devices and networks used to connect to KCJIS are kept apart from them.

Remember that because none of us can control what is in the air it is considered "other external networks" in KCJIS policy 5.10.1.1. 3 and must be separated from your trusted wired network by a firewall.

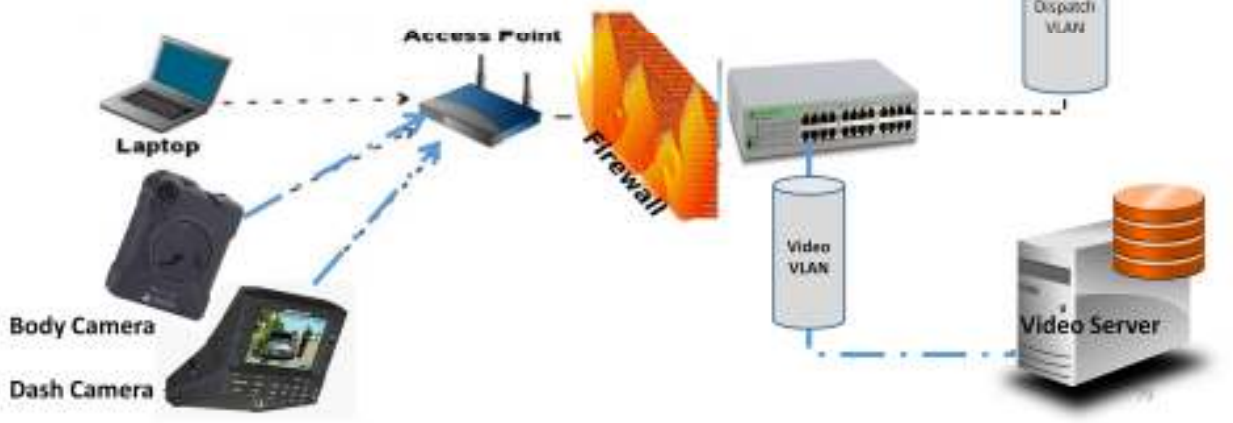
Devices connected wirelessly must also have their own firewall or reasonable alternative we'll discuss shortly.

5.13 Policy Area 13: Mobile Devices (+ Appendix G.4)

5.13.1.1 802.11 Wireless Protocols

Agencies shall implement the following controls for all agency-managed wireless ***access points with access to an agency's network that processes unencrypted CJI***:

15. Insulate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. ***Limit access between wireless networks and the wired network to only operational needs.***



While the FBI CJIS APB process is not currently pursuing any policies specific to body worn or in car video cameras and their data.

Keep in mind that the INFRASTRUCTURE used to transfer audio and video recordings from mobile devices into network area storage systems is subject to the CJSI security policy as are any connections into an information system (network) used to process, transmit or store CJI.

The freedom of no wires opens new frontiers for security considerations. Devices can't just be classified by their **form factor**. Desktops now come with wireless communication. Does it have a real keyboard? How easy is it to conceal if someone wanted to take it, or for the authorized user to loose it?

Operating systems have changed. Traditional ***"Full Featured" operating systems*** are loaded with feature sets that manage all applications installed on the device and allow one app to share data and resources with other apps. Most of them also allow multiple users to share data and resources on the device. Features come with a need for controlling who can access what.
"Limited Functionality" operating systems generally don't allow apps to share resources. Applications are usually installed through the OS vendor's "store", not from manual install files or enterprise downloads. They have limited built in storage capacity, are VERY dependent on connectivity across the air to get or save data or to receive instructions and permission for operations. They also are designed for single users. Because of these and other basic design traits, they typically need to be managed differently than your Windows 7 desktop.

Another consideration is the wireless **connectivity**. If it is not able to communicate, it won't be able to be managed the same way wired devices are.
802.11 only means it is dependent on another device to connect. Is it always connected to the internet via cellular? Does it have a combination of both? Who can "disconnect" it?

5.13 Policy Area 13: Mobile Devices (+ Appendix G.4)

Managing devices accessing your network and CJI

5.13.2 Mobile Device Management (MDM)

- ❑ CJI only transferred between authorized applications and storage
- ❑ Centralized administration
  - ❑ Remote Lock
  - ❑ Remote Wipe
  - ❑ Setting and locking device configuration
  - ❑ Detect rooted or jailbroken
  - ❑ Enforce encryption (5.10.1.2)
  - ❑ Apply policies
  - ❑ Detect unauthorized configurations

Enter Mobile Device Management.

Primarily used to manage devices running Limited Functionality operating systems

A novice comparison is to say Mobile Device Management is to limited functionality operating systems as directory services group policies are to full featured operating systems.

Limited functionality devices with MDM setup MUST have a way to connect to the MDM server to get instructions and permissions to run apps.
MDM controls what the device can (or can't) do.
Its restrictive controls are near equivalent to a personal firewall on the device.
Its ability to interrogate the connecting device for misbehaving apps offer similar protections to your network as traditional anti-virus software on a full feature O.S.
Policy lists the things an MDM must be able to do to protect CJI.

Remember ALL devices used to access CJI are subject to the same levels of required protections.

5.13 Policy Area 13: Mobile Devices (+ Appendix G.4)

Managing devices accessing your network and CJI

5.5.6.1 Personally Owned Information Systems

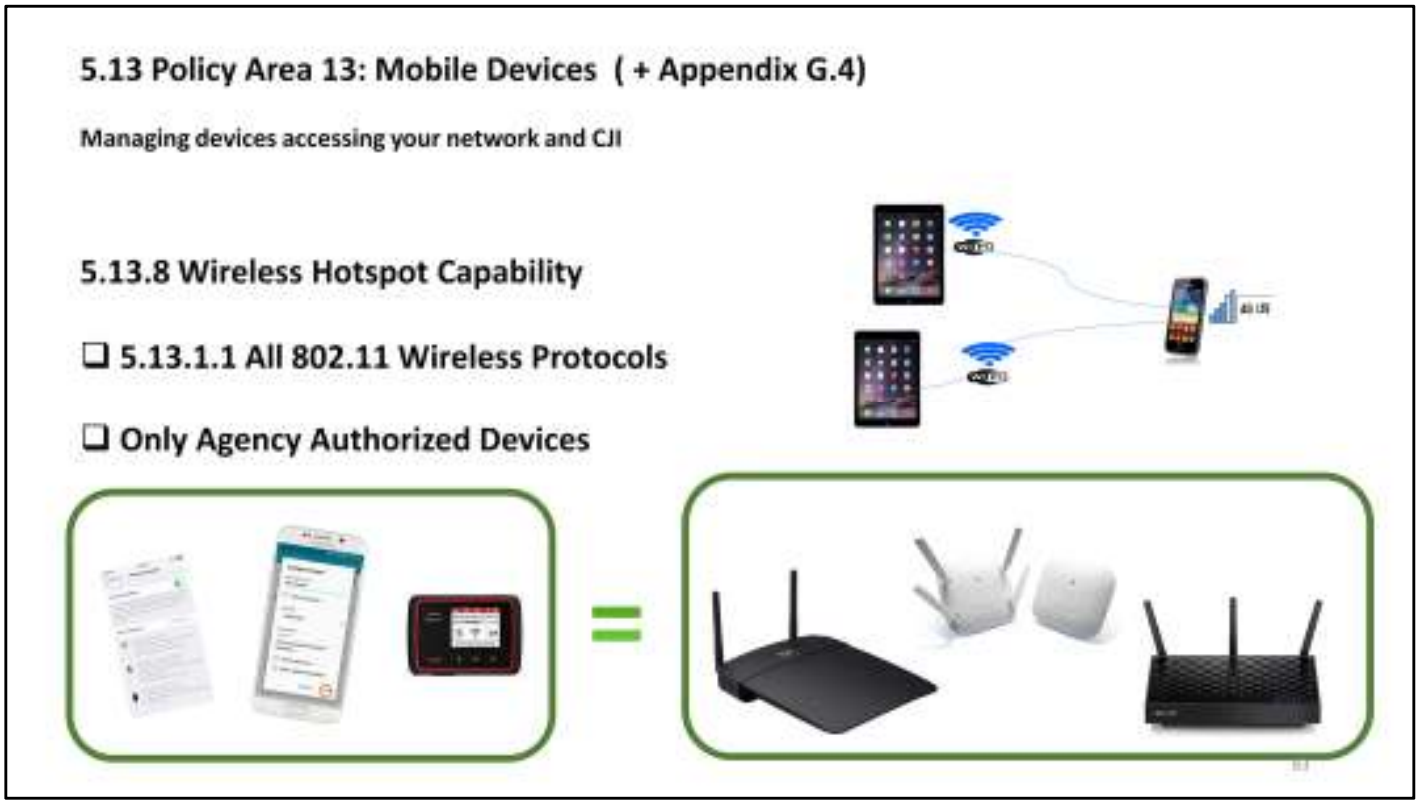
When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices.

Which brings us to those wonderfully tech savvy employees who want to use their own smartphone to access your RMS system, etc.

Policy does not specifically prohibit it. But it comes pretty close!
Unless the agency HAS documented all the specifics terms and strings attached for such use, the answer is NO. Those attached strings are policy area 5.13.
5.13 has other strings tying it back to other policy areas, like 5.5 Access control, and 5.6 identification and authentication, and 5.10, etc.

So when that tech savvy officer request use of their own device – document how they can do it and thank them for the generosity.
Because they essentially just donated a $ 650 smartphone to the agency.

(p.s. CJIS security policy doesn't even scratch into legal concerns regarding discovery or other issues that may result from its use for “official business” .
Just ask a certain former Secretary of State!)



As cellular and smartphone technologies have evolved, a newer feature has allowed the parallel use of cellular and 802.11 wireless technologies.

Some phones now offer capabilities for internet access over 802.11 to save on cellular data consumption.

The reverse of that is to offer use of the phone's cellular connection to other lesser equipped devices for internet access.

Be sure the smartphones can be configured like a bigger wireless access point into your wired network (5.13.1.1):

- ❑ Password protect the smartphone's settings to 5.6.2. 1 levels
- ❑ Disguise the Service Set Identifier (SSID) so the folks in the coffee shop can't tell it belongs to the agency.
- ❑ Don't broadcast the SSID, (even better - so those folks can't even see it as they search for free internet!)
- ❑ Encryption still applies!
- ❑ Etc.
- ❑ Etc.
- ❑ Etc.


HAPPY TRAILS TO YOU